UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
(Doutorado)

DOUGLAS FERNANDO COPATTI

CÓDIGOS QUÂNTICOS TOPOLÓGICOS SOBRE TESSELAÇÕES HIPERBÓLICAS SEMIRREGULARES [1]

Maringá-PR

2022

[1]O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

CÓDIGOS QUÂNTICOS TOPOLÓGICOS SOBRE TESSELAÇÕES HIPERBÓLICAS SEMIRREGULARES

TESE DE DOUTORADO

DOUGLAS FERNANDO COPATTI

Tese apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Doutor em Matemática.
Área de concentração: Matemática Aplicada

Orientador: Prof. Dr. Eduardo Brandani da Silva

Maringá
2022

Dados Internacionais de Catalogação-na-Publicação (CIP)
(Biblioteca Central - UEM, Maringá - PR, Brasil)

C781c

Copatti, Douglas Fernando

Códigos quânticos topológicos sobre tesselações hiperbólicas semirregulares / Douglas Fernando Copatti. -- Maringá, PR, 2022.

111 f.: il. color., figs., tabs.

Orientador: Prof. Dr. Eduardo Brandani da Silva.

Tese (Doutorado) - Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento de Matemática, Programa de Pós-Graduação em Matemática, 2022.

1. Códigos quânticos corretores de erros. 2. Códigos quânticos topológicos. 3. Computação quântica. 4. Códigos coloridos. 5. Códigos de superfície. I. Silva, Eduardo Brandani da, orient. II. Universidade Estadual de Maringá. Centro de Ciências Exatas. Departamento de Matemática. Programa de Pós-Graduação em Matemática. III. Título.

CDD 23.ed. 003.54

Elaine Cristina Soares Lira - CRB-9/1202

DOUGLAS FERNANDO COPATTI

CÓDIGOS QUÂNTICOS TOPOLÓGICOS SOBRE TESSELAÇÕES HIPERBÓLICAS SEMIRREGULARES

Tese apresentada ao Programa de Pós-Graduação em Matemática do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Doutor em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Prof. Dr. Eduardo Brandani da Silva - UEM (Presidente)
Prof. Dr. Edson Donizete de Carvalho - UNESP
Prof. Dr. Waldir Silva Soares Junior - UTFPR/Pato Branco
Prof. Dr. Emerson Vitor Castelani - UEM
Prof. Dr. Francisco Nogueira Calmon Sobral - UEM

Aprovado em: 23 de novembro de 2022.
Local de defesa: Videoconferência – Google Meet (https://meet.google.com/utz-nmei-buq)

André Luiz Marques

(in memoriam)

Agradecimentos

Gostaria de agradecer à minha família, em especial à minha esposa Alana e à minha filha Lívia, por todo o apoio, incentivo, paciência e confiança que em mim depositaram durante todos estes anos;

Ao meu orientador, Eduardo Brandani da Silva, por toda ajuda, incentivos e conselhos que me forneceu durante todo este tempo. Pessoa grandiosa e paciente, além de orientador, é um grande amigo e conselheiro;

A todos os meus amigos e colegas de doutorado, que quero levar para a vida toda;

A todos os meus grandes amigos por todo o apoio que me deram;

Aos professores que compuseram a banca da presente tese, pelo tempo doado à leitura, correção e melhora do presente trabalho;

Aos professores do programa de pós-graduação em Matemática da Universidade Estadual de Maringá, em especial aos que contribuíram para a minha formação acadêmica;

Ao Instituto Federal do Paraná, em especial aos meus colegas de trabalho, pelo apoio para que eu pudesse dar andamento ao doutorado da melhor forma possível;

À Universidade Estadual de Maringá, e em especial ao seu Programa de Pós Graduação em Matemática, pela oportunidade e, finalmente, à CAPES pelo suporte e incentivo financeiro disponibilizado no início desta caminhada, sem os quais a presente pesquisa não poderia ser desenvolvida.

Resumo

Um código quântico de superfície é aquele que utiliza tesselações sobre superfícies compactas e conexas como ferramenta para a construção do grupo estabilizador, visto que são casos particulares dos códigos estabilizadores. Esta construção oferece um tratamento geométrico à análise dos códigos estabilizadores assim obtidos. Tal tratamento geométrico possibilita a obtenção de um limitante inferior para a distância do código. Mais ainda, por serem também casos particulares de códigos topológicos, cada operador do grupo estabilizador atua numa pequena quantidade de qubits do espaço do código, o que permite a implementação de uma computação tolerante à falhas: Pode-se construir um hardware com uma determinada taxa de erros em cada componente sem que estes condenem o processamento como um todo.

Como primeiro resultado deste trabalho, destacamos a construção de códigos de superfície provenientes de tesselações semirregulares estabelecidas sobre superfícies compactas, conexas e orientáveis cuja característica de Euler é negativa. Como se sabe, estas superfícies são canonicamente munidas de uma métrica hiperbólica e possuem curvatura negativa. Este fato nos permite obter uma infinidade de tesselações semirregulares, de qualquer valência, em detrimento das poucas possibilidades que o caso euclidiano permite.

Os códigos coloridos, que são construídos de forma muito similar aos de superfície, porém substancialmente mais ricos em propriedades, também ganham aqui o seu tratamento a partir de tesselações semirregulares estabelecidas sobre superfícies compactas, conexas e orientáveis cuja característica de Euler é negativa. Assim como no caso construído com tesselações regulares, existe uma infinidade de tesselações semirregulares 3-valentes e 3-coloríveis. Cada uma destas nos fornece um código quântico colorido. Estes, por se tratarem de casos particulares de códigos topológicos, também compõem o escopo dos códigos quânticos corretores de erros que permitem uma computação tolerante à falhas.

Abstract

A surface quantum code is one that uses tessellations on compact and connected surfaces as a tool for the construction of the stabilizer group, since these are particular cases of the stabilizer codes. This construction offers a geometric treatment for the analysis of the stabilizer codes thus obtained. Such geometric treatment makes it possible to obtain a lower bound for the code distance. Furthermore, as they are also particular cases of topological codes, it follows that each operator of the stabilizer group acts in a limited amount of code space qubits, which allows the implementation of fault-tolerant computing: that is, you can build hardware with a certain error rate in each component without them condemning the processing as a whole. As a first result of this work, we highlight the construction of surface codes from semi-regular tessellations established on compact, connected and orientable surfaces whose Euler characteristic is negative. As is known, these surfaces are canonically provided with a hyperbolic metric and have negative curvature. This fact allows us to obtain an infinity of semiregular tessellations, of any valence, to the detriment of the few possibilities that the Euclidean case allows. Color codes, which are constructed in a very similar way to surface codes, but substantially richer in properties, also gain their treatment here from the semi-regular tessellations established on compact, connected and orientable surfaces whose Euler characteristic is negative. As in the case constructed with regular tessellations, there are an infinity of 3-valent and 3-colorable semiregular tessellations. Each of these gives us a color quantum code. These, as they are specific cases of topological codes, also compose the scope of the error correcting quantum codes that allow a fault tolerant computation.

Introdução

A primeira descrição do que foi o embrião para nossos computadores atuais foi dada por Alan M. Turing, em seu notável trabalho [54], de 1936. Nele, Turing descreve o que hoje conhecemos por computador programável, através de um modelo abstrato de computação, hoje conhecida como Máquina de Turing, em sua homenagem. Turing mostrou que existe uma Máquina de Turing Universal, capaz de simular qualquer outra máquina de Turing.

Turing e Alonzo Church, independentemente em [54, 18, 17], afirmam que a universalidade de uma máquina de Turing é absoluta, no sentido de que para qualquer algoritmo capaz de ser processado por um computador, existe um algoritmo equivalente para a Máquina de Turing Universal, que a faz desenvolver as mesmas tarefas que o primeiro. Esta é a famosa Hipótese de Church-Turing, cujo nome homenageia os dois grandes nomes da ciência da computação.

Pouco tempo depois da publicação do trabalho de Turing, o primeiro computador começa a ser desenvolvido a partir de um modelo teórico elaborado por John Von Newmann, o qual descreve um protótipo para a implementação de uma máquina de Turing concreta, desenvolvida por componentes eletrônicos, a qual foi constantemente aperfeiçoada, principalmente pela criação dos transistores, até se tornarem os computadores que conhecemos hoje.

Em meados de 1947, Richard Wesley Hamming trabalhava no Laboratório Bell de Tecnologias. Este laboratório, assim como muito poucas instituições à época, possuíam um computador, o qual era programado através de cartões perfurados. Estas máquinas já contavam com tecnologia suficiente para abortar uma rotina de processamento e partir para a próxima, sempre que algum erro ocorresse. Hamming tinha acesso restrito a estes computadores[2], e por diversas vezes acabou encontrando os seus trabalhos não finalizados, em decorrência do aparecimento de algum erro computacional. Esta situação o levou a estabelecer o primeiro

[2]Alguns autores, como [43], dizem que este acesso era liberado somente aos finais de semana.

código corretor de erros, [36]. Este feito ocorreu em 1947, porém a publicação deste resultado só viera a ocorrer em 1950, em virtude de o laboratório pedir a patente do código. Durante estes três anos, Hamming indagava, em memorandos internos de seu laboratório, a respeito da existência de códigos corretores de erros mais eficientes do que aquele que encontrara. A resposta foi dada, indiretamente, por Claude Elwood Shannon, na segunda metade do ano de 1948, [45], publicado no mesmo jornal que mais tarde receberia a publicação de Hamming.

O trabalho de Shannon deu início a dois novos campos de pesquisa à época, a saber, a teoria de códigos corretores de erros e a teoria da informação, respectivamente.

Junta-se a estes dois nomes o de Marcel J.E. Golay. Golay encontrou importantes códigos corretores de erros, [33], os quais basearam outros códigos corretores de erros, que mais tarde viabilizariam a viajem espacial do projeto Voyager, mais especificamente no processo de envio eficaz de imagens do espaço, desde o espaço, na ocasião capturadas.

Um código corretor de erros é, em síntese, uma maneira organizada de se acrescentar algum grau de redundância a uma informação que se necessita transmitir, de modo que se esta eventualmente for acometida de algum erro, este possa ser detectado e corrigido. Para obter melhor eficiência no processo de transmissão de informação, o grau de redundância, bem como a quantidade de erros que podem ser detectados e/ou corrigidos dependem das especificidades do canal de transmissão e são estabelecidos pela escolha do código.

Exatamente no ano de 1947, John Bardeen, Walter Brattain e Will Shockley desenvolveram o primeiro transistor. Desde então o aperfeiçoamento de hardware dos computadores tem tido um crescimento exponencial, literalmente, o qual foi notado por Gordon Moore, no que ficou conhecida como Lei de Moore: A cada dois anos, os computadores dobram a seu poder de processamento, mantendo-se constante o custo, tanto de espaço quanto de consumo.

Em 1982, Paul Benioff, [7], descreve um primeiro modelo de computação, baseado na cinemática e dinâmica quânticas, porém, este ainda era efetivamente clássico, no sentido computacional estabelecido em [27]. Em 1982, Richard P. Feynman, [31], propõe o primeiro modelo de computador baseado nos princípios da mecânica quântica, que mais se aproximou de um simulador quântico universal. Em 1983, David Z. Albert, [1], descreve uma forma de automação no processo de medição quântica, que por ele observado, não possuem análogo na

computação clássica. Em 1985, David Deutsch, [27], apresenta um modelo completamente quântico de computação, no formato de uma versão quântica para a Máquina de Turing.

Deutsch indagava se é possível para um computador quântico resolver eficientemente problemas que não possuem solução eficiente na computação clássica. Ele então construiu um simples exemplo sugerindo que, de fato, computadores quânticos tem um poder de computação maior do que os clássicos. Este importante (primeiro) passo dado por D. Deutsch, que foi aprimorado na década subsequente por diversos pesquisadores, culminou no trabalho de Peter Shor,[47], em 1994: Este mostrara que dois problemas muito importantes poderiam ser resolvidos eficientemente por um computador quântico, a saber, o Problema do Logaritmo Discreto e o Problema da Decomposição em Fatores Primos de um Número Inteiro. Acredita-se que estes dois problemas não tenham solução eficiente no âmbito da computação clássica. Este trabalho é, portanto, um importante indicativo de que computadores quânticos são, de fato, mais poderosos computacionalmente do que os clássicos.

William Unruh, [55], alertou que uma computação quântica padece sob o efeito do decaimento quântico[3]. Para contornar o efeito nocivo da decoerência, formas de computação quântica tolerante à falhas são necessárias. Um meio para tal feito reside nos códigos quânticos corretores de erros. Um código quântico corretor de erros é uma ferramente matemática utilizada para codificar estados físicos de sistemas quânticos utilizando algum nível de redundância, de forma que a informação contida em tal estado, mesmo passando por um processo de ruído, possa ser, após o processo que se chama de decodificação, retomada.

O primeiro código quântico corretor de erros do qual se tem registro foi exibido por Shor em 1995, [47]. Este foi concebido utilizando-se uma concatenação de dois códigos de 3 qubits, os quais são os códigos quânticos corretores de erros bit-flip e phase-shift, respectivamente.

No ano seguinte surgiu na literatura uma construção de códigos quânticos corretores de erros, que viria a generalizar as que até então estavam estabelecidas. Hoje os conhecemos por códigos CSS, que é um acrônimo derivado dos sobrenomes de seus idealizadores, a saber, Robert Calderbank, Peter Shor e Andrew Steane, [52], [14]. Na esteira desta descoberta,

[3]A decoerência de um estado quântico, de um sistema físico é, em síntese, o efeito da interação deste sistema com o seu exterior. A decoerência afeta um estado quântico em superposição, fazendo-o colapsar. Sem a superposição de estados, a computação é essencialmente clássica.

Daniel Gottesman desenvolve uma nova generalização dos códigos CSS, os chamados códigos estabilizadores, [34], que nada mais são do que subespaços vetoriais de um espaço de Hilbert $\mathcal{H}$, estabilizados por um subgrupo do seu grupo de operadores lineares, que possui algumas propriedades específicas. Este grupo é chamado de grupo estabilizador.

Um caso particular dos códigos estabilizadores, e que devemos destacar aqui como sendo a semente para o trabalho que aqui estamos desenvolvendo, foi proposto por Alexei Kitaev [40], e atualmente são conhecidos como códigos quânticos topológicos. Uma das grandes vantagens do código proposto por Kitaev é a de que os elementos do grupo estabilizador são geometricamente locais, com suporte relativamente pequeno, composto por alguns poucos qubits concentrados numa vizinhança poligonal, num determinado sentido.

Em [23], foi proposto uma extensão dos códigos de Kitaev para superfícies com gênero maior que um, usando ferramentas da geometria hiperbólica. Neste contexto, Albuquerque, Pallazo e Silva utilizaram tesselações hiperbólicas para obter códigos de superfície com os melhores parâmetros dentre os códigos topológicos existentes na literatura à época.

Em 2016, Terhal e Breuckmann, [13], fizeram uma abordagem semelhante à de [23], utilizando superfícies de gênero maior que um, munidas de uma métrica hiperbólica e, adicionalmente, obtiveram estimativas numéricas para o valor do limiar de erro e da probabilidade de erro lógico desses códigos contra ruídos independentes, do tipo $\mathfrak{X}$ ou $\mathfrak{Z}$. Este estudo leva em consideração que a correção de erro seja realizada completamente sem ruído.

Bombin e Martin-Delgado, [9], propuseram uma subclasse dos códigos quânticos estabilizadores, que ficou conhecido na literatura como códigos quânticos coloridos. Os códigos quânticos coloridos também são códigos topológicos, como os de Kitaev, mas com um elemento extra na rotulação, a cor. Uma vantagem imediata dos códigos coloridos é que codificam o dobro de qubits que os códigos de superfície, em relação a uma mesma superfície.

Por fim, recentemente em [50], Soares e Silva juntaram a construção dos códigos de superfície baseados na geometria hiperbólica de [21] com a construção dos códigos coloridos de [9] e obtiveram códigos coloridos provenientes de tesselações regulares 3-valente e 3-coloríveis do g-toro, $g \geq 2$.

Proposta da Tese

Dentre os códigos quânticos corretores de erros, destacaremos os códigos estabilizadores e destes, destacaremos os códigos topológicos. Um código quântico topológico faz uso de uma certa liberdade topológica para as palavras código. Dentro desta classe, vamos nos atentar à família dos códigos de superfície. Num primeiro momento, este trabalho se propõe a utilizar técnicas semelhantes às de Albuquerque, Pallazo e Silva, [23], sobre os códigos de superfície, desenvolvendo novos códigos quânticos de superfície associados, porém, à tesselações semirregulares de superfícies hiperbólicas.

Posteriormente, tendo em vista os códigos coloridos descobertos por Bombim e Martin-Delgado, [8], e a construção sobre tesselações regulares de superfícies hiperbólicas introduzidas por Waldir Soares Jr, [50, 51], apresentaremos uma nova família de códigos coloridos, agora associados à tesselações semirregulares de superfícies hiperbólicas.

A figura 1 traz um fluxograma dos tópicos cuja compreensão é necessária para chegarmos ao escopo deste nosso trabalho.

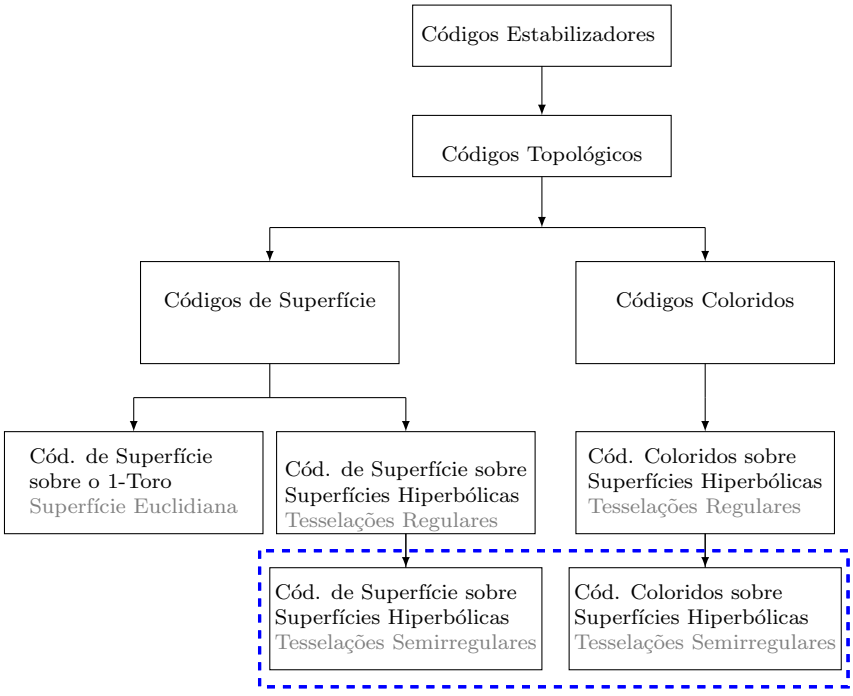


Figura 1: Fluxograma ilustrando a sequência de tópicos que são prerrequisitos para a compreensão do cerne deste trabalho, o qual está destacado no retângulo azul tracejado.

Descrição da Tese

No **1º capítulo** desta tese apresentamos os conceitos fundamentais para o seu desenvolvimento, relembrando conceitos úteis e fixando notações. Já no **2º capítulo**, apresentamos alguns elementos da mecânica quântica, em dose não mais que suficiente para o seu uso posterior, levantando alguns fatos interessantes desta teoria ao presente texto.

No **3º capítulo** apresentamos alguns dos códigos quânticos a fim de dar base à nossa posterior construção. Neste capítulo foram explorados os códigos Bit Flip e Phase Shift, de Shor e o de Steane, bem como os códigos conhecidos na literatura por CSS, os quais derivam de códigos clássicos corretores de erros. Com um passo adiante, na direção do cerne deste trabalho, apresentamos os códigos estabilizadores e, como subconjunto desta classe, os códigos topológicos. Dentre os códigos topológicos, destacam-se os códigos de superfície e os códigos coloridos, construídos a partir de tesselações hiperbólicas regulares de uma superfície compacta, orientável e conexa, munida de uma métrica hiperbólica - o g-toro, com $g \geq 2$.

No **4º capítulo**, apresentamos uma nova construção de famílias de códigos de superfície, baseada agora em tesselações hiperbólicas semirregulares do g-toro, com $g \geq 2$.

Finalmente, no **5º capítulo** apresentamos uma nova construção de famílias de códigos coloridos, baseada agora em tesselações hiperbólicas semirregulares do g-toro, com $g \geq 2$.

Sumário

Capítulo 1

Conceitos Fundamentais

1.1 Códigos Clássicos Corretores de Erros

Com o intuito de situar o leitor e fixar as notações, nesta seção vamos discorrer brevemente sobre códigos clássicos corretores de erros[1]. Para mais detalhes acerca disto, indicamos [38].

O exemplo mais trivial de um código corretor de erros é, sem dúvidas, um idioma. A fim de ilustrar isso, vamos tomar como exemplo a língua portuguesa. Para tal, considere $\mathcal{A}$, o conjunto constituído pelas 23 letras do alfabeto, juntamente com o conjunto de todas as vogais acentuadas, cedilha e o espaço. O conjunto $\mathcal{A}$ é constituído por todos os caracteres necessários para a escrita de qualquer palavra da língua portuguesa. Do ponto de vista dos códigos, este é chamado de Alfabeto, ou simplesmente de conjunto de caracteres do código.

Uma palavra do idioma é um elemento de $\mathcal{A}^{46}$, onde o expoente 46 é obtido pela quantidade de caracteres da maior palavra deste idioma[2]. Obviamente, nem todas as palavras de $\mathcal{A}^{46}$ fazem parte do idioma. Denotemos por $\mathbb{P}$ o conjunto das palavras do idioma em pauta.

Ilustrando a afirmação feita acerca de que um idioma é um código corretor de erros, suponha que ao escrevermos uma determinada palavra, escrevamos a sequencia de caracteres "cathorro". É fácil notar que a palavra que desejávamos escrever é "cachorro". A detecção de erro, neste caso, consiste em notar que a palavra "cathorro"não pertence ao idioma $\mathbb{P}$, enquanto que a correção do erro consiste na interpretação desta como sendo "cachorro".

Conforme observado em [38], sob a ótica da detecção e correção de erros, este código não

[1]Com o advento da computação quântica e, em especial, dos códigos quânticos corretores de erros, faz-se necessária a distinção entre computação clássica e quântica.

[2]Com 46 letras, pneumoultramicroscopicossilicovulcanoconiótico descreve indivíduo que possui doença pulmonar causada pela inspiração de cinzas vulcânicas.

é eficiente. Podemos facilmente ilustrar isso considerando a situação em que a palavra "gato" seja escrita erroneamente como "pato", "rato"ou "galo". Esta falta de eficiência ocorre pois, por exemplo, estas quatro palavras estão muito próximas, sob uma métrica inerente aos códigos, conhecida na literatura por Métrica de Hamming: A Métrica de Hamming em $\mathcal{A}^n$ é definida por $d(u,v) = \#\{i, u_i \neq v_i; 1 \leq i \leq n\}$, para cada $u = (u_i)_i$, $v = (v_i)_i \in \mathcal{A}^n$.

Um código corretor de erros é um subconjunto próprio de $\mathcal{A}^n$, onde $\mathcal{A}$ é um conjunto finito e não vazio, denominado conjunto de caracteres, ou mesmo alfabeto do código, enquanto que o inteiro positivo n é chamado de comprimento do código. Denotaremos $q = \#\mathcal{A}$.

O trato da informação é realizado, basicamente, sobre três pilares: fonte, canal e destinatário. A fonte é o agente emissor da informação, enquanto que o canal é o meio pelo qual tal informação é enviada ou armazenada e, por fim, o destinatário é o agente final do processo, o qual recebe a informação e dá os devidos encaminhamentos, conforme sua finalidade.

Consideremos, para fins didáticos, que exista um robô comandado remotamente, que se move pelas casas contíguas de um tabuleiro de xadrez, nas direções Norte(N)/Sul(S) e Leste(E)/Oeste(W), uma casa por vez. Para controlar os movimentos do referido robô, dentre as várias opções, podemos estabelecer a codificação de fonte descrita no quadro abaixo:

$N \leftrightarrow 00$	$S \leftrightarrow 01$	$E \leftrightarrow 10$	$W \leftrightarrow 11$

Essa codificação leva o adjetivo "de fonte", visto que o emissor da mensagem realiza a mesma. A informação proveniente do comando executado pelo operador deste robô, após codificada, precisa ser acrescida de uma determinada redundância, para possibilitar a correção de erros. Neste passo estaremos implementando a codificação de canal, a qual é realizada de sorte que os (a maioria dos) erros que possam incidir sobre a informação transmitida, no canal de transmissão, sejam posteriormente detectados e corrigidos. Para fins de ilustração, estaremos supondo que o canal utilizado exponha o dado transmitido a, no máximo, um erro em um bit[3]. Desta maneira podemos codificar, novamente, o comando do operador. Agora com um certo grau de redundância, de forma que possamos identificar e corrigir erros.

Segue abaixo uma possível maneira de realizar tal feito:

[3]bit é a unidade básica de informação clássica, obtida pela utilização do alfabeto $\{0,1\}$.

$$\begin{aligned} N &\rightarrow 00 \rightarrow 00000 \\ S &\rightarrow 01 \rightarrow 01011 \\ E &\rightarrow 10 \rightarrow 10101 \\ W &\rightarrow 11 \rightarrow 11110 \end{aligned}$$

Suponha agora que o comando executado pelo operador deste robô seja o deslocamento de uma casa para o sentido sul. A respectiva codificação de fonte é 01, enquanto que a informação a ser enviada pelo canal é 01011. Suponha, momentaneamente, que a informação recebida pelo destinatário seja 00011. Num primeiro momento, verifica-se que esta palavra, 00011, não é uma palavra pertencente ao código. Detecta-se, deste modo, a existência de um erro. Utilizando a métrica de Hamming, verifica-se que a palavra pertencente ao código, que é mais próxima desta palavra recebida, é a palavra 01011. Isto nos permite inferir que ocorreu um erro no segundo bit, e que a palavra que deveria ser recebida pelo robô é 01011.

Utilizando uma decodificação, a qual aqui é fácil de estabelecer, o robô executará o comando correto: Tal decodificação consiste, por exemplo, na escolha da palavra-código mais próxima, sob o ponto de vista da métrica de Hamming, da palavra recebida.

Segue abaixo uma ilustração do processo da transmissão ou armazenamento da informação.

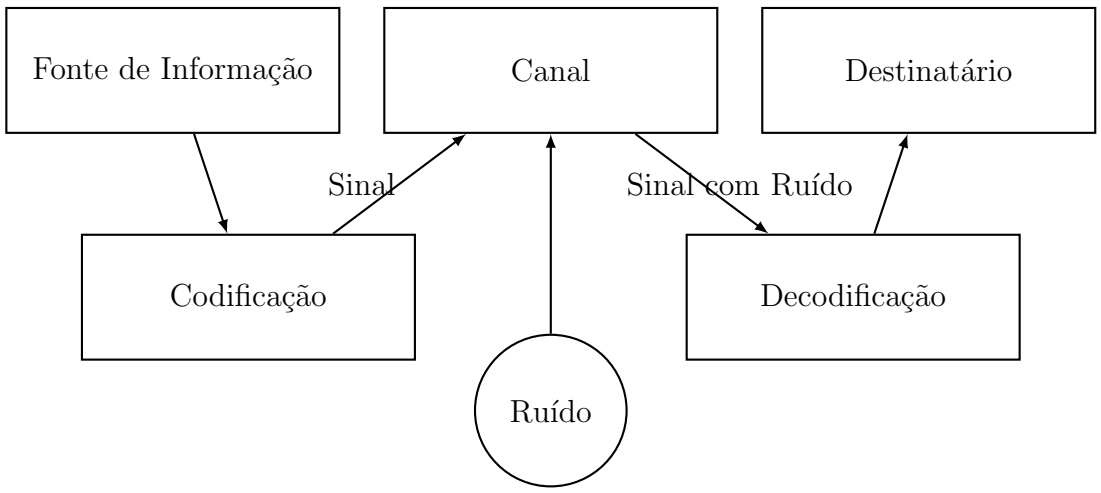


Figura 1.1: Fluxograma do processo de transmissão ou armazenamento de informação.

1.1.1 Códigos Lineares

Dentre todo o espectro de formas de implementar um código clássico, a classe que oferece maior praticidade e, portanto, é mais comumente utilizada na prática é a dos códigos lineares. Estes, em síntese, são os códigos cujo conjunto de caracteres é munido de uma estrutura de corpo finito e o conjunto das palavras-código constituem um espaço vetorial sobre o mesmo.

O interesse do presente trabalho em introduzir os conceitos básicos acerca dos códigos lineares reside na posterior utilização como ferramenta indispensável para a confecção dos códigos quânticos CSS, que são explorados mais adiante, na seção 3.6. Essa é a justificativa para estudarmos aqui apenas os códigos lineares sobre $\mathbb{Z}_2$. Evidenciamos, apesar disto, a existência de uma grande gama de códigos lineares sobre corpos de característica finita.

Um código linear $\mathcal{C}$ que codifica k bits de informação em n bits, é um subespaço vetorial de $\mathbb{Z}_2^n$. Este código $\mathcal{C}$ é dito um $[n,k]$-código linear e pode ser completamente determinado[4] por uma matriz $G \in M_{n\times k}(\mathbb{Z}_2)$, chamada de Matriz Geradora. Dada a identificação entre matrizes e transformações lineares, podemos escrever $G : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$, $x \mapsto Gx$. Aqui podemos perceber que o código fonte é estabelecido através da matriz G, sua matriz geradora.

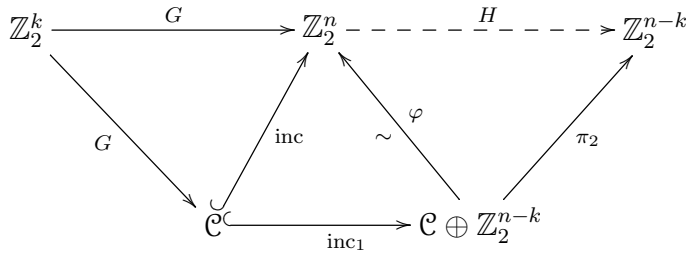
Exemplo 1.1.1. O código de repetição é um código linear. O Código de repetição é aquele que codifica k bits em $n = kr$ bits e é descrito pela matriz $G = \begin{pmatrix} Id_k \\ \vdots \\ Id_k \end{pmatrix}$, a qual é composta por r blocos da matriz identidade de ordem k.

É importante notar que se G é uma matriz $n \times k$, que é a matriz geradora de um código $\mathcal{C}$, então $k < n$. Tendo em vista que o espaço vetorial das palavras código é o gerado pelas colunas de G, e que a codificação de canal é obtida pela multiplicação de G pelo vetor proveniente da codificação da fonte, é necessário que G tenha posto máximo para que tal codificação seja feita de forma única, no sentido de que duas palavras distintas, codificadas na fonte, são recodificadas em elementos distintos. Portanto, doravante vamos considerar, sem perda de generalidade, que a transformação linear $G : \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ é injetiva.

Considere $\mathcal{C}$ um $[n,k]$-código linear, cuja matriz geradora é G. Tem-se $\mathcal{C} = Im(G)$. Con-

[4]Estamos considerando implicitamente que foram fixadas bases dos espaços e subespaços envolvidos.

sidere, adicionalmente, a inclusão canônica $\text{inc} : \mathcal{C} \to \mathbb{Z}_2^n$, a inclusão na primeira coordenada $\text{inc}_1 : \mathcal{C} \to \mathcal{C} \oplus \mathbb{Z}_2^{n-k}$, a qual é definida por $\text{inc}_1(x) = (x, \bar{0})$, e o isomorfismo $\varphi : \mathcal{C} \oplus \mathbb{Z}_2^{n-k} \to \mathbb{Z}_2^n$, o qual é definido por $\varphi(c \oplus v) = (c, 0) + (0, v)$. Se $\pi_2 : \mathcal{C} \oplus \mathbb{Z}_2^{n-k} \to \mathbb{Z}_2^{n-k}$, tal que $\pi_2(c, z) = z$, é a projeção canônica na segunda coordenada, considere a transformação linear $H : \mathbb{Z}_2^n \to \mathbb{Z}_2^{n-k}$ como sendo a única transformação linear que completa o diagrama abaixo:



Observação 1.1.2. Dado $c \in \mathcal{C}$, $H(c) = H(c + 0) = H \circ \varphi(c \oplus 0) = \pi_2(c \oplus 0) = 0$. Reciprocamente, se $\pi_1 : \mathcal{C} \oplus \mathbb{Z}_2^{n-k} \to \mathcal{C}$ é a projeção canônica na primeira coordenada, podemos escrever, $0 = H(v) = H \circ \varphi(c \oplus w) = \pi_2(c \oplus w) = w$, onde $v \in Ker(H)$, é tal que $\varphi(c \oplus w) = v$. Feito isso, é simples e conveniente perceber que $\mathcal{C} = Ker(H)$.

A matriz H é chamada de Matriz de Verificação de Paridade do Código $\mathcal{C}$. Esta matriz é empregada no processo de verificação acerca de uma palavra recebida pelo destinatário ser, ou não, uma palavra código. Note que um dado vetor $v \in \mathbb{Z}_2^n$ pertence ao código $\mathcal{C}$ se, e só se, o sistema linear $Gx = v$ possui solução. Sob a ótica do custo computacional, é menos custoso verificar se Hv é o vetor nulo de $\mathbb{Z}_2^{n-k}$, em detrimento de verificar se $Gx = v$ possui alguma solução. Chamamos de Síndrome de erros de um vetor $v \in \mathbb{Z}_2^n$ ao vetor $H(v)$.

Exemplo 1.1.3. O código de Hamming de ordem m sobre $\mathbb{Z}_2$ é o código linear cuja matriz de verificação de paridade H é constituída por todos os vetores não nulos do espaço $\mathbb{Z}_2^m$, numa ordem qualquer. Considerando que $\mathbb{Z}_2^m$ possui exatamente $2^m - 1$ elementos não nulos, ao organizar estes vetores em colunas de uma matriz H, obtemos uma matriz de $M_{m \times n}(\mathbb{Z}_2)$, com $n = 2^m - 1$. Uma construção alternativa da matriz de verificação de paridade de um código de Hamming parte de notar que cada uma de suas colunas é determinada pela sequência de dígitos de cada número $j = 1, \cdots, 2^m - 1$ no sistema binário. Como exemplo disto, ilustramos a seguir uma matriz de verificação de paridade do código de Hamming de ordem 3, H_3:

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

O peso do vetor u, onde $u \in \mathbb{Z}_2^n$, é definido por $\omega(u) = d(u, 0)$. A distância (mínima) de um código linear $\mathcal{C}$ é o menor peso positivo obtido dentre os vetores de $\mathcal{C}$. Designa-se por $[n, k, d]$-código linear todo $[n, k]$-código linear $\mathcal{C}$, cuja distância mínima é d. O peso de um vetor assim definido é conhecido como peso de Hamming e a distância, por consequência, é conhecida como distância de Hamming do código.

Decodificação e Síndrome de Erros de um Código Linear

O processo de detecção e correção de erros de um código $\mathcal{C}$ é chamado de decodificação. Neste processo, a diferença entre o vetor recebido pelo destinatário, em relação ao enviado pela fonte, é chamado de (um) padrão de erro. O seguinte teorema fornece um importante resultado acerca dos padrões de erro. Para obter mais detalhes sobre, indicamos [38].

Teorema 1.1.4. *Um código clássico corretor de erros cujos parâmetros são $[n, k, d]$ é capaz de detectar até $d - 1$ erros e é capaz de corrigir até $t = \left\lceil \frac{d-1}{2} \right\rceil$ erros.*[5]

A relação de equivalência induzida no espaço Z_2^n pelo seu quociente por $\mathcal{C}$ determina uma partição de $\mathbb{Z}_2^n$, onde cada classe corresponde a um único padrão de erros. Para fins de maior clareza podemos listar esse fenômeno numa tabela, chamada de arranjo padrão. Para tal, considere $\mathcal{C} = \{0 = v_1, v_2, \cdots, v_{2^k}\}$. Assim sendo, existem 2^{n-k} padrões de erros, os quais denotaremos, respectivamente, por $e_1, \cdots, e_{2^{n-k}}$. O Arranjo padrão, nesta ocasião, é:

[5] $\lceil \cdot \rceil$ denota a função máximo inteiro

$$\begin{array}{cccccc}
v_1 = 0 & v_2 & \cdots & v_j & \cdots & v_{2^k} \\
e_1 & v_2 + e_1 & \cdots & v_j + e_1 & \cdots & v_{2^k} + e_1 \\
e_2 & v_2 + e_2 & \cdots & v_j + e_2 & \cdots & v_{2^k} + e_2 \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
e_i & v_2 + e_i & \cdots & v_j + e_i & \cdots & v_{2^k} + e_i \\
\vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\
e_{2^{n-k}} & v_2 + e_{2^{n-k}} & \cdots & v_j + e_{2^{n-k}} & \cdots & v_{2^k} + e_{2^{n-k}}
\end{array}$$

Observação 1.1.5. Assume-se, na construção do arranjo padrão, sem perda de generalidade, que $\omega(e_i) \leq \omega(v_j + e_i)$, $j = 1, \cdots, v_{2^k}$. O vetor e_i é chamado de vetor líder da classe $e_i + \mathcal{C}$.

Percebe-se que cada vetor de $\mathbb{Z}_2^n$ está listado exatamente uma vez no arranjo padrão, bem como que cada linha deste arranjo corresponde a uma única classe de equivalência de $\mathbb{Z}_2^n/\mathcal{C}$.

Suponha que uma mensagem codificada em um vetor $v \in \mathcal{C}$ é acometida de um erro e_i, de forma que a mensagem a ser decodificada é $v + e_i$. Como $\mathcal{C} = Ker(H)$, segue que para cada $i = 1, \cdots, 2^{n-k}$, $H(v + e_i) = H(e_i)$. Tomando o vetor líder da pré imagem de $v + e_i$, constata-se qual é o padrão de erros pelo qual a informação original foi corrompida. Da maneira como foi construído o arranjo padrão, tem-se $H(e_a) \neq H(e_b)$, sempre que $a \neq b$.

Um processo de decodificação, conhecido na literatura como Decodificação por Máxima Verossimilhança, é descrito pelo fluxograma da figura 1.2 a seguir.

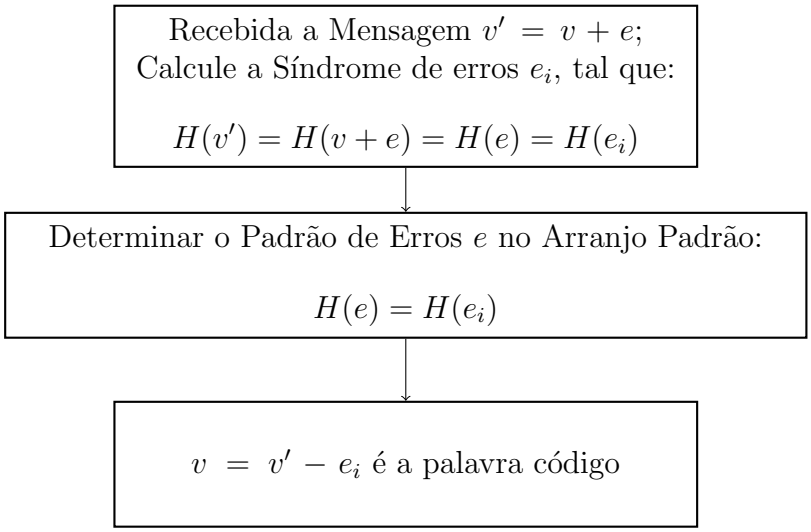


Figura 1.2: Fluxograma: Decodificação por Máxima Verossimilhança

Códigos Duais

A noção de código dual, além de estabelecer uma maneira de construção de códigos clássicos desde códigos já conhecidos, nos será útil ao estabelecermos os códigos CSS, na seção 3.6.

Ao considerar o produto interno formal $\langle u, v\rangle = \sum u_i v_i$ definido em $\mathbb{Z}_2^n$, chama-se de Código Dual de um código $\mathcal{C}$, ao código $\mathcal{C}^\perp$, definido por:

$$\mathcal{C}^\perp = \{u \in \mathbb{Z}_2^n / \langle u, v\rangle = 0,\ \forall v \in \mathcal{C}\}.$$

O primeiro fato a constatar-se acerca dos códigos duais é que se $\mathcal{C}$ é um código linear em $\mathbb{Z}_2^n$, de dimensão k, então $\mathcal{C}^\perp$ é um código linear de dimensão $n-k$, [38].

Parâmetros de Qualidade de um Código

Dentre diversos parâmetros de qualidade de um código, vamos salientar os limitantes de Hamming e de Singleton. Para este último, faz-se necessário o teorema que segue, cuja demonstração pode ser obtida em [38].

Teorema 1.1.6. *Seja $\mathcal{C}$ um $[n,k]$-código linear, cuja matriz de verificação de paridade é H. A distância mínima de $\mathcal{C}$ é d se, e somente se, quaisquer $d-1$ colunas de H são linearmente independentes e existem d colunas linearmente dependentes.*

Agora, se $\mathcal{C}$ é um $[n,k,d]$-código linear, com matriz de verificação de paridade H, tem-se que o posto de H é $d-1$. Visto que $H(\mathbb{Z}_2^n) \subset \mathbb{Z}_2^{n-k}$, segue que $d-1 \leq n-k$. Essa desigualdade comumente aparece na literatura como $d \leq n-k+1$, e é chamada de Limitante de Singleton. Um $[n,k,d]$-código que satisfaz com igualdade o limitante de Singleton é aquele que possui a distância máxima possível para um $[n,k]$-código. Por este motivo, é comumente designado por MDS (Maximum Distance Separable).

Teorema 1.1.7 (Limitante de Hamming)**.** *Se $\mathcal{C}$ é um $[n,k,d]$-código linear sobre $\mathbb{Z}_2$, que corrige até t erros, então, se $m = \#\mathcal{C}$, vale a seguinte relação:*

$$m\left(1 + \binom{n}{1} + \cdots + \binom{n}{t}\right) \leq 2^n.$$

1.2 Fundamentos Algébricos

Esta seção é utilizada para fixar notações e listar resultados algébricos utilizados no presente texto. Os espaços de Hilbert de dimensão finita são de grande interesse no âmbito da física quântica pois, como veremos mais adiante, um sistema físico, em escala quântica, pode ser modelado por um espaço de Hilbert com estas qualidades. Veremos adiante que o sistema físico mais elementar é modelado por (um subconjunto de) $\mathbb{C}^2$ e que qualquer sistema físico composto é modelado por produtos tensoriais destes primeiros.

A notação de Dirac é empregada para denotar, no âmbito da física, vetores de um espaço de Hilbert: Para cada vetor u pertencente a um espaço de Hilbert $\mathcal{H}$, escolhe-se um símbolo φ_u, e denota-se $u = |\varphi_u\rangle$. Os vetores de um espaço de Hilbert serão denominados, eventualmente, por "estados". A notação de Dirac é largamente utilizada dentro da mecânica quântica, a qual, por sua vez, permeia o presente trabalho. Esta notação é chamada de "ket".

Um produto interno Hermitiano estabelecido em um espaço de Hilbert $\mathcal{H}$ é uma aplicação $\langle \cdot \mid \cdot \rangle : \mathcal{H}^2 \to \mathbb{C}$, sujeito às seguintes condições, para todo $u, v, w \in \mathcal{H}, \lambda \in \mathbb{C}$:

a. $\langle u \,|v\rangle = \langle v \,|u\rangle^*$;

b. $\langle u + w \,|v\rangle = \langle u \,|v\rangle + \langle w \,|v\rangle$;

c. $\langle \lambda u \,|v\rangle = \lambda \,\langle u \,|v\rangle = \langle u \,|\lambda^* v\rangle$;

d. $\langle \lambda u \,|u\rangle > 0$, sempre que $u \neq 0$.

Observação 1.2.1. i. Denota-se o conjugado complexo de $x \in \mathbb{C}$ por x^*.

ii. Utiliza-se a notação $\langle\varphi|$ para denotar a aplicação $\langle\varphi| \cdot\rangle : \mathcal{H} \to \mathbb{C}$. Em termos matriciais, $\langle\varphi|$ é o transposto conjugado de $|\varphi\rangle$, isto é, $\langle\varphi| = |\varphi\rangle^\dagger$.

Um operador linear M é dito hermitiano se sua representação matricial é hermitiana, isto é, $M[i,j] = M[j,i]^*$. Um operador (matriz) M é dito unitário quando $M^\dagger = M^{-1}$.

Exemplo 1.2.2 (Matrizes de Pauli)**.** São exemplos de matrizes hermitianas e unitárias as matrizes de Pauli, definidas a seguir:

$$\sigma_0 = Id = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \sigma_1 = \mathfrak{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\sigma_2 = \mathfrak{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_3 = \mathfrak{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Exemplo 1.2.3. Operadores que são hermitianos e/ou unitários:

a. O operador de Hadammard, $\mathfrak{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, é hermitiano e unitário;

b. O operador Fase, $\mathfrak{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, é unitário, mas não hermitiano;

c. O operador $\frac{\pi}{8}$, $\mathfrak{T} = \begin{pmatrix} 1 & 0 \\ 0 & exp(i\pi/4) \end{pmatrix}$, é unitário, mas não hermitiano.

O colchete (de Lie) dos operadores A, B é $[A, B] = AB - BA$. Analogamente, define-se $\{A, B\} = AB + BA$. Diz-se que A e B comutam se $[A, B] = 0$ ou anticomutam se $\{A, B\} = 0$.

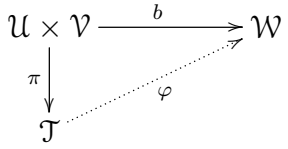
Seja $\mathcal{A}$ um anel comutativo, com unidade, e $(\mathcal{V}, +)$ um grupo abeliano. Considere a aplicação $\cdot : \mathcal{A} \times \mathcal{V} \to \mathcal{V}$, definida por $\cdot(a, v) = a \cdot v$. Suponha adicionalmente que, independentemente da escolha de $a, b \in \mathcal{A}$ e $u, v \in \mathcal{V}$, ocorre $(a+b) \cdot (u+v) = a \cdot u + a \cdot v + b \cdot u + b \cdot v$, $(ab) \cdot v = a \cdot (b \cdot v)$ e que $1 \cdot v = v$. Dizemos, satisfeitas tais hipóteses, que $\mathcal{V}$ é um $\mathcal{A}$-módulo.[6]

Por mais que a noção de módulos seja muito abrangente, nos restringiremos apenas aos conceitos fundamentais para o nosso texto. Devemos observar que, a menos de isomorfismo de módulos, não há necessidade em fazer referência quanto a lateralidade da estrutura de módulo quando o anel subjacente é comutativo. A noção de módulos é uma generalização natural de espaços vetoriais. Para mais detalhes, indicamos as referências [3], [42] ou [46].

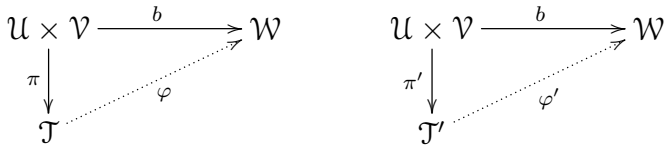
Os módulos de nosso principal, mas não exclusivo interesse, são os de matrizes complexas, sobre o corpo $\mathbb{C}$, dos números complexos. Os módulos mais utilizados neste trabalho, porém, são os (produtos tensoriais de) espaços complexos 2-dimensionais.

[6] tecnicamente, $(\mathcal{V}, +, \mathcal{A}, \cdot)$ é um módulo.

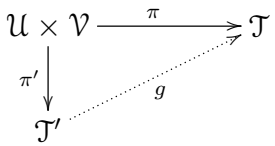
Dados dois $\mathcal{A}$-módulos quaisquer $\mathcal{U}$ e $\mathcal{V}$, existe um par $(\mathcal{T}, \pi)$, constituído por um $\mathcal{A}$-módulo $\mathcal{T}$ e por uma aplicação $\mathcal{A}$-bilinear $\pi : \mathcal{U} \times \mathcal{V} \to \mathcal{T}$, que possuem a seguinte propriedade, a qual é comumente conhecida como Propriedade Universal do Produto Tensorial: dado qualquer $\mathcal{A}$-módulo $\mathcal{W}$ e qualquer aplicação $\mathcal{A}$-bilinear $b : \mathcal{U} \times \mathcal{V} \to \mathcal{W}$, existe uma única aplicação $\mathcal{A}$-linear $\varphi : \mathcal{T} \to \mathcal{W}$ que faz o seguinte diagrama comutar:



Proposição 1.2.4. Sejam $\mathcal{U}, \mathcal{V}$ $\mathcal{A}$-módulos, $(\mathcal{T}, \pi)$ e $(\mathcal{T}', \pi')$, onde $\mathcal{T}, \mathcal{T}'$ são $\mathcal{A}$-módulos e $\pi : \mathcal{U} \times \mathcal{V} \to \mathcal{T}$ e $\pi' : \mathcal{U} \times \mathcal{V} \to \mathcal{T}'$ são aplicações $\mathcal{A}$-bilineares. Suponha que, dado qualquer $\mathcal{A}$-módulo $\mathcal{W}$ e uma aplicação $\mathcal{A}$-bilinear $b : \mathcal{U} \times \mathcal{V} \to \mathcal{W}$, existem únicas aplicações $\mathcal{A}$-linear $\varphi : \mathcal{T} \to \mathcal{W}$ e $\varphi' : \mathcal{T}' \to \mathcal{W}$ que fazem os seguintes diagramas comutarem



Sob estas hipóteses, existe um único isomorfismo de $\mathcal{A}$-módulos $g : \mathcal{T}' \to \mathcal{T}$, que faz o seguinte diagrama comutar:



A proposição acima nos diz que, a menos de isomorfismo de $\mathcal{A}$-módulos, existe um único par $(\mathcal{T}, \pi)$ que completa aquele diagrama. Isto nos permite definir tal módulo por produto tensorial de $\mathcal{U}$ e $\mathcal{V}$ e denotar o mesmo por $\mathcal{U} \otimes \mathcal{V}$. A aplicação $\pi : \mathcal{U} \times \mathcal{V} \to \mathcal{U} \otimes \mathcal{V}$ é dada, a menos de uma extensão $\mathcal{A}$-linear, por $(u, v) \mapsto u \otimes v$. A construção que garante a existência de um produto tensorial de dois módulos já é estabelecida na literatura, podendo ser encontrada na maioria dos textos de álgebra comutativa, por exemplo. Nestes, vê-se que um produto tensorial é um quociente especial de módulos, definidos *ad hoc*.

Um exemplo de grande valia para o nosso trabalho, que pode ser encontrado também em [44], é o chamado Produto de Kronecker, que estabelece o (a projeção associada ao) produto

tensorial de duas matrizes sobre o mesmo anel de escalares: Se $\mathcal{A}$ é um anel comutativo, com unidade, $A = [a_{ij}]_{ij} \in M_{m\times n}(\mathcal{A})$, $B = [b_{ij}]_{ij} \in M_{p\times q}(\mathcal{A})$, então o produto tensorial de A por B, nesta ordem, é uma matriz de ordem $mp \times nq$, descrita por mn blocos de dimensão $p \times q$, e cujo bloco que ocupa a i-ésima linha e a j-ésima coluna de blocos é dado como segue:

$$[A \otimes B]_{ij} = [a_{ij}B]_{ij}$$

Exemplo 1.2.5. Sejam $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ e $B = \begin{pmatrix} 7 & 8 & 9 \end{pmatrix}$. O produto tensorial $A \otimes B$, entre A e B, é:

$$\begin{aligned} A \otimes B &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \otimes \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} \\ &= \begin{pmatrix} 1 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} & 2 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} \\ 3 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} & 4 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} \\ 5 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} & 6 \cdot \begin{pmatrix} 7 & 8 & 9 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} \begin{pmatrix} 07 & 08 & 09 \end{pmatrix} & \begin{pmatrix} 14 & 16 & 18 \end{pmatrix} \\ \begin{pmatrix} 21 & 24 & 27 \end{pmatrix} & \begin{pmatrix} 28 & 32 & 36 \end{pmatrix} \\ \begin{pmatrix} 35 & 40 & 45 \end{pmatrix} & \begin{pmatrix} 45 & 48 & 54 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} 7 & 8 & 9 & 14 & 16 & 18 \\ 21 & 24 & 27 & 28 & 32 & 36 \\ 35 & 40 & 45 & 42 & 48 & 54 \end{pmatrix} \end{aligned}$$

Suponha que $\mathcal{V}$ é um espaço vetorial e que E é um operador de $\mathcal{V}$. Consideremos o produto tensorial $\mathcal{V}_1 \otimes \mathcal{V}_2 \otimes \cdots \otimes \mathcal{V}_n$, onde $\mathcal{V}_j = \mathcal{V}$. Define-se a aplicação $E_j : \mathcal{V}^{\otimes^n} \to \mathcal{V}^{\otimes^n}$ da seguinte maneira:

$$E_j = \underbrace{Id \otimes Id \otimes \cdots \otimes Id \otimes}_{j-1 fatores} E \underbrace{\otimes Id \otimes Id \otimes \cdots \otimes Id}_{n-j fatores}.$$

Exemplo 1.2.6. Se $\mathcal{V} = \mathbb{C}^2$, os operadores listados abaixo atuam sobre $\mathcal{V}^3$:

a. $\mathfrak{X}_1 = \mathfrak{X} \otimes Id \otimes Id$ b. $\mathfrak{X}_2 = Id \otimes \mathfrak{X} \otimes Id$ c. $\mathfrak{X}_3 = Id \otimes Id \otimes \mathfrak{X}$

Exemplo 1.2.7 (Grupo de Pauli)**.** Fixada uma base de $\mathbb{C}^2$, cada matriz de Pauli é canonicamente associada a um operador linear. Desta maneira, dado $n \in \mathbb{N}$, pode-se construir o grupo de Pauli $\mathcal{P}_n$, gerado pelos operadores $\{\mathfrak{X}_j, \mathfrak{Y}_k, \mathfrak{Z}_l\}_{j,k,l=1,\cdots,n}$. Este grupo é chamado de Grupo de Pauli de n qubits. Os elementos do Grupo de Pauli são operadores Hermitianos.

O peso de um elemento do grupo de Pauli é exatamente a quantidade de qubits que estão em seu suporte, isto é, se $g = \prod_{j=1}^{n} \mathfrak{X}_j^{x_j} \mathfrak{Y}_j^{y_j} \mathfrak{Z}_j^{z_j}$, o seu peso é $\omega(g) = \sum_{j=1}^{n} \delta\left((x_j + y_j + z_j) > 0\right)$.

Observação 1.2.8. Dada uma proposição p, estabelecemos a notação (função) $\delta(p)$:

$$\delta(p) = \begin{cases} 1 & \text{, se p é verdadeira} \\ 0 & \text{, se p é falsa} \end{cases}.$$

Considere um espaço de Hilbert $\mathcal{H}$, munido de um produto interno hermitiano $\langle \cdot \mid \cdot \rangle$. Dados $|v\rangle, |w\rangle \in \mathcal{H}$, o produto exterior dos vetores $|v\rangle$ e $|w\rangle$ é o operador linear $|v\rangle\langle w|$ de $\mathcal{H}$, definido por $|v\rangle\langle w| = \langle w| \cdot \rangle |v\rangle$. Fixada a base $\{|0\rangle, |1\rangle\}$ de $\mathbb{C}^2$, podemos escrever:

$$\begin{aligned} \mathfrak{X} &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ \mathfrak{Y} &= i|1\rangle\langle 0| - i|0\rangle\langle 1| \\ \mathfrak{Z} &= |0\rangle\langle 1| - |1\rangle\langle 0| \\ \mathfrak{H} &= \frac{|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|}{\sqrt{2}} \end{aligned}$$

Observação 1.2.9. Frequentemente, na ausência de possibilidade de confusão, utilizaremos a notação $|\varphi\psi\rangle$, ou mesmo $|\varphi, \psi\rangle$, ao nos referirmos ao produto tensorial $|\varphi\rangle \otimes |\psi\rangle$.

1.3 Grupos e Ações de Grupos Sobre Módulos

O centralizador de um subgrupo $\mathcal{G} < \mathcal{H}$ é o conjunto $\mathcal{C}(\mathcal{G}) = \{h \in \mathcal{H}; gh = hg, \forall g \in \mathcal{G}\}$, enquanto que o normalizador de $\mathcal{G}$ é o conjunto $\mathcal{N}(\mathcal{G}) = \{h \in \mathcal{H}; hgh^{-1} \in \mathcal{G}, \forall g \in \mathcal{G}\}$.

Se $\mathcal{P}_n$ é o grupo de Pauli de n qubits, e $\mathcal{G} < \mathcal{P}_n$ é um subgrupo qualquer, é possível mostrar que $\mathcal{C}(\mathcal{G}) = \mathcal{N}(\mathcal{G})$. Este fato é largamente utilizado na construção dos códigos

quânticos corretores de erros e, em especial, na construção dos códigos estabilizadores.

Dizemos que um grupo $\mathcal{G}$ age sobre $\mathcal{X}$ se existe uma aplicação $\Phi : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$, tal que $\Phi_g \equiv \Phi(g, \cdot) : \mathcal{X} \to \mathcal{X}$ é uma bijeção, tal que se $g, h \in \mathcal{G}$, tem-se $\Phi_g \circ \Phi_{h^{-1}} = \Phi_{gh^{-1}}$. Denotamos $\Phi_g(x) = gx$. A ação é livre de pontos fixos se $gx \neq x$, para cada $g \in \mathcal{G}$ e $x \in \mathcal{X}$, com $g \neq Id_{\mathcal{G}}$. Se $\mathcal{X}$ é um espaço topológico, a ação é propriamente descontínua se, para cada $x \in \mathcal{X}$, existe uma vizinhança $V_x \ni x$, tal que $gV_x \cap V_x = \emptyset$, para cada $g \in \mathcal{G}$, com $g \neq Id_g$.

O subgrupo estabilizador de um elemento $x \in \mathcal{X}$, ou o grupo de isotropia de x, é o grupo $G_x = \{g \in \mathcal{G}/gx = x\}$, enquanto que subgrupo estabilizador, ou de isotropia de um subconjunto $\mathcal{X}' \subset \mathcal{X}$ é o grupo definido por $\mathcal{G}_{\mathcal{X}'} = \{g \in \mathcal{G}/gx = x, \forall x \in \mathcal{X}'\}$. Obviamente este grupo é obtido pela intersecção do grupos estabilizadores de cada $x \in \mathcal{X}'$. O subconjunto $\mathcal{X}'$ é dito estabilizado por $\mathcal{G}_{\mathcal{X}'}$. A órbita de um elemento $x \in \mathcal{X}$ é o conjunto $\mathcal{G}x = \{gx/g \in \mathcal{G}\}$.

1.4 Fundamentos da Geometria Hiperbólica

Os postulados de Euclides constituem os pontos mais primordiais no estudo da geometria euclidiana. Estes foram escritos por volta dos anos 300 a.C. e, durante muito tempo, foram tacitamente aceitos. Num determinado momento passou-se a indagar se o quinto postulado, o das paralelas, era, ou não, consequência dos demais. Desde Euclides, quase dois mil anos se passaram até que Gauss mostrou a existência de uma geometria consistente, onde os quatro primeiros postulados, mas não o quinto, eram válidos. Sobre esta descoberta, Gauss escreve algo equivalente a: "Assumir que a soma dos ângulos internos de um triângulo é menor do que 180°, permite estabelecer uma geometria diferente daquela de Euclides, mas ainda consistente". Este foi o primeiro exemplo de geometria não-Euclidiana. Gauss nunca publicou seu achado. Contudo, de maneira independente, Lobachevsky, em 1829, e Bolay em 1832, redescobriram esta geometria, a qual atualmente conhecemos por Geometria Hiperbólica.

Além deste fato eventualmente curioso, não nos atentaremos demasiadamente aos detalhes desta geometria. Para estes, e como leitura complementar, indicamos [39, 6, 5, 2].

O Disco de Poincaré é o conjunto $\mathbb{D} = \{z \in \mathbb{C}; |z| < 1\}$, munido com a métrica $ds = \frac{2|dz|}{1-|z|^2}$.

Considere, para cada $\alpha, \beta \in \mathbb{C}$, tais que $|\alpha|^2 - |\beta|^2 = 1$, a aplicação $\gamma : \mathbb{D} \to \mathbb{D}$, dada

por $\gamma(z) = \dfrac{\alpha z + \beta}{\bar{\beta} z + \bar{\alpha}}$. Esta aplicação é chamada de Transformação de Möbius. O conjunto $M\ddot{o}b(\mathbb{D})$, das transformações de Möbius, é um grupo cuja operação subjacente é a composição de aplicações. Cada Transformação de Möbius é uma aplicação conforme. Uma aplicação conforme é aquela que preserva ângulos e distâncias.

Observação 1.4.1. i. Considere $\gamma : \mathbb{D} \to \mathbb{C}^2$, tal que $\gamma(z) = \dfrac{\alpha z + \beta}{\bar{\beta} z + \bar{\alpha}}$. Se $\alpha = 0$, então $|\alpha|^2 - |\beta|^2 = -|\beta|^2 < 0$. Isto implica que $\gamma \notin M\ddot{o}b(\mathbb{D})$.

ii. Seja $\gamma : \mathbb{D} \to \mathbb{D}$, definida por $\gamma(z) = \dfrac{\alpha z + \beta}{\bar{\beta} z + \bar{\alpha}}$. Note que $\dfrac{\alpha z + \beta}{\bar{\beta} z + \bar{\alpha}} = \dfrac{-\alpha z - \beta}{-\bar{\beta} z - \bar{\alpha}}$. Portanto, sem perda de generalidades podemos considerar que $\alpha > 0$.

O grupo $M\ddot{o}b(\mathbb{D})$ tem uma métrica canônica: Dados quaisquer $\gamma_i(z) = \frac{\alpha_i z + \beta_i}{\bar{\beta}_i z + \bar{\alpha}_i} \in M\ddot{o}b(\mathbb{D})$, $\alpha_i > 0$, $i = 1, 2$, tem-se $dist(\gamma_1, \gamma_2) = \big|\big|(\alpha_1, \beta_1, \bar{\beta}_1, \bar{\alpha_1}) - (\alpha_2, \beta_2, \bar{\beta}_2, \bar{\alpha_2})\big|\big|$. Um subgrupo Γ de $M\ddot{o}b(\mathbb{D})$ é dito um Grupo Fuchsiano se é discreto, em relação à topologia induzida pela métrica de $M\ddot{o}b(\mathbb{D})$.

Teorema 1.4.2 (Adaptado de [39])**.** *Um subgrupo $\Gamma \subset M\ddot{o}b(\mathbb{D})$ é um grupo Fuchsiano se, e somente se, atua propriamente descontinuamente sobre $\mathbb{D}$.*

Corolário 1.4.3 (Adaptado de [39])**.** Um subgrupo $\Gamma \subset M\ddot{o}b(\mathbb{D})$ atua propriamente descontinuamente sobre $\mathbb{D}$ se, e somente se, a órbita de qualquer elemento $z \in \mathbb{D}$ é um subconjunto discreto de $\mathbb{D}$.

Proposição 1.4.4. Seja Γ um subgrupo de $M\ddot{o}b(\mathbb{D})$. São equivalentes:

i. Γ é discreto (Fuchsiano);

ii. Id_Γ é um elemento isolado;

iii. A órbita de cada $z \in \mathbb{D}$ é um subconjunto discreto de $\mathbb{D}$.

Demonstração: $(i \Rightarrow ii)$ Se Γ é discreto, obviamente Id_Γ é um elemento isolado.

$(ii \Rightarrow i)$ Se Id_Γ é um elemento isolado, então $\{Id_\Gamma\}$ é aberto em Γ. Dada qualquer $\gamma \in M\ddot{o}b(\mathbb{D})$, considere $\Phi_{\gamma^{-1}} : M\ddot{o}b(\mathbb{D}) \to M\ddot{o}b(\mathbb{D})$, dada por $\Phi_{\gamma^{-1}}(\varphi) = \gamma^{-1}\varphi$.

Independentemente da escolha de $\gamma \in M\ddot{o}b(\mathbb{D})$, $\Phi_{\gamma^{-1}}$ é uma aplicação contínua. Portanto, $\{\gamma\} = \Phi^{-1}_{\gamma^{-1}}\{Id_\Gamma\}$ é aberto em Γ. Logo, γ é um elemento isolado.

$(i \Leftrightarrow iii)$ Decorre da aplicação do teorema 1.4.2 juntamente com o Corolário 1.4.3.□

O traço de uma transformação de Möbius $\gamma \in M\ddot{o}b(\mathbb{D})$ que é dada por $\gamma(\cdot) = \frac{\alpha \cdot + \beta}{\bar{\beta} \cdot + \bar{\alpha}}$, é definido por $\tau(\gamma) = \left[tr \begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \bar{\alpha} \end{pmatrix} \right]^2 = (\alpha + \bar{\alpha})^2$. Uma transformação de Möbius não trivial γ é classificada em parabólica, elíptica ou hiperbólica se $\tau(\gamma)$ é igual, menor, ou maior do que quatro, respectivamente. As transformações de Möbius que nos interessam são as elípticas.

As transformações elípticas são conjugadas a uma rotação do disco de Poincaré $z \mapsto e^{i\theta} z$.

Observação 1.4.5. Daqui em diante consideraremos apenas polígonos hiperbólicos cujos vértices se situam no interior de $\mathbb{D}$. Mais detalhes sobre este assunto são encontrados em [6].

Teorema 1.4.6. *Considere um triângulo hiperbólico cujos ângulos internos medem α, β e $\frac{\pi}{2}$. Adicionalmente, considere que a, b e c são os comprimentos hiperbólicos dos lados oposto a α, β e $\frac{\pi}{2}$, respectivamente. São válidas as seguintes relações:*

$$\cosh(c) = \cosh(a)\cosh(b), \tag{1.1}$$

$$\operatorname{tgh}(b) = \operatorname{senh}(a)\operatorname{tg}(\beta), \tag{1.2}$$

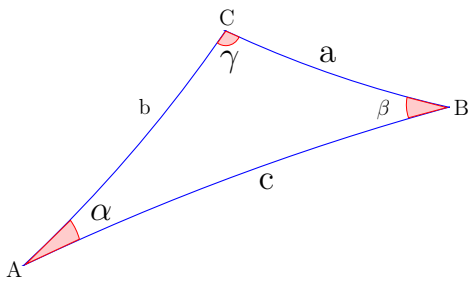
$$\operatorname{senh}(b) = \operatorname{senh}(c)\operatorname{sen}(\beta), \tag{1.3}$$

$$\operatorname{tgh}(a) = \operatorname{tgh}(c)\cos(\beta), \tag{1.4}$$

$$\cos(\alpha) = cosh(a)\operatorname{sen}(\beta), \tag{1.5}$$

$$\cosh(c) = \operatorname{cotg}(\alpha)\operatorname{cotg}(\beta). \tag{1.6}$$

Teorema 1.4.7. *Considere um triângulo hiperbólico de vértices A, B e C, cujos ângulos internos medem α, β e γ, respectivamente, e cujos respectivos lados opostos medindo a, b e c.*



São validas as seguintes relações:

i. A Lei dos Senos para Triângulos Hiperbólicos:

$$\frac{\operatorname{senh}(a)}{\operatorname{sen}(\alpha)} = \frac{\operatorname{senh}(b)}{\operatorname{sen}(\beta)} = \frac{\operatorname{senh}(c)}{\operatorname{sen}(\gamma)} \tag{1.7}$$

ii. A 1ª Lei dos Cossenos para Triângulos Hiperbólicos:

$$\cosh(c) = \cosh(a)\cosh(b) - \operatorname{senh}(a)\operatorname{senh}(b)\cos(\gamma) \tag{1.8}$$

iii. A 2ª Lei dos Cossenos para Triângulos Hiperbólicos:

$$\cosh(c) = \frac{\cos(\alpha)\cos(\beta) + \cos(\gamma)}{\operatorname{sen}(\alpha)\operatorname{sen}(\beta)} \tag{1.9}$$

Lema 1.4.8. Considere um triângulo cujos lados medem a, b e c, com os respectivos ângulos opostos medindo α, β e γ. O raio R, da circunferência inscrita neste triângulo, pode ser obtido através da relação

$$\tanh^2(R) = \frac{\cos^2(\alpha) + \cos^2(\beta) + \cos^2(\gamma) + 2\cos(\alpha)\cos(\beta)\cos(\gamma) - 1}{2(1+\cos(\alpha))(1+\cos(\beta))(1+\cos(\gamma))}.$$

Um dos resultados da geometria hiperbólica de maior elegância matemática é expresso pelo teorema de Gauss-Bonnet. Este, assim como as fórmulas trigonométricas hiperbólicas, fornecem informações acerca de polígonos baseado apenas em seus ângulos internos, eventualmente desconsiderando o comprimento de lado dos mesmos.

Teorema 1.4.9 (Gauss-Bonnet para Triângulos Hiperbólicos)**.** *Um triângulo hiperbólico de ângulos internos medindo α, β e γ tem área igual a $\pi - (\alpha + \beta + \gamma)$.*

Visto que um n-gon de ângulos internos $\alpha_1, \cdots, \alpha_n$ pode ser decomposto em n triângulos, segue que a área deste é dada por $(n-2)\pi - \sum_j \alpha_j$.

1.5 Tesselações

Fixado um ponto $P \in \mathbb{D}$, um polígono hiperbólico $\mathbb{P}$ que contém P é uma interseção finita de semiplanos que contém P. Um lado de um polígono $\mathbb{P}$ é uma aresta munida de uma orientação. Dado um grupo Fuchsiano Γ, uma Região Fundamental para este é um subconjunto aberto $F \subset \mathbb{D}$, que possui as seguintes propriedades:

i. $\bigcap_{\gamma \in \Gamma} \gamma(\bar{F}) = \mathbb{D}$;

ii. As imagens de F via elementos de Γ são duas a duas disjuntas.

A família $\{\gamma(F); \gamma \in \Gamma\}$ é chamada uma tesselação de $\mathbb{D}$. A tesselação é dita Regular se F é um polígono regular.

De maneira geral, uma tesselação de uma superfície $\mathbb{M}$ é, em síntese, o recobrimento desta por meio de polígonos regulares, que satisfazem as condições abaixo:

i. Não há sobreposição de polígonos, isto é, estes possuem os interiores dois a dois disjuntos;

ii. Na eventualidade de dois polígonos se intersectarem, tal intersecção se dá ao longo de aresta (s) inteira(s) ou em vértice(s).

Suponha que, dado um vértice v de uma determinada tesselação, este pertença a exatamente t polígonos desta, cada um dos quais é um p_j-gon, com $j = 1, \cdots, t$, considerando o sentido horário ou anti-horário. Dizemos, então, que t é a Valência de v e que $[p_1, \cdots, p_t]$ é o Tipo de Vértice de v. O tipo de vértice não percebe permutações cíclicas em seus índices. Uma tesselação é dita semirregular se todos os seus vértices são de um mesmo tipo. Uma tesselação semirregular é dita regular se, adicionalmente, todos os polígonos subjacentes são congruentes. Denotamos uma uma tesselação regular, cujos polígonos que constituem as faces são p-gons e cuja valência de cada vértice é q, simplesmente por $\{p, q\}$.

O Incentro de um polígono P, quando existe, é o centro da circunferência inscrita a este. Chamamos de apótema de um polígono regular ao comprimento do raio da circunferência nele inscrita. O teorema 1.5.1 contempla a existência do incentro de um polígono.

Teorema 1.5.1 (adaptado de [6]). *Sejam $\theta_1, \cdots, \theta_t$ números reais, tais que $0 \leq \theta_j < \pi$, para cada $j = 1, \cdots, t$. Existe um polígono hiperbólico P, cujos ângulos internos medem, nesta ordem e a menos de uma permutação cíclica, $\theta_1, \cdots, \theta_t$, se e somente se, $\sum_j \theta_j < (t-2)\pi$. Nestas condições existe uma circunferência inscrita no polígono P.*

Observação 1.5.2. A prova do teorema 1.5.1 é feita construindo-se um quadrilátero Q_j, para cada $j = 1, \cdots, t$, cujo ponto O indicado é a origem, conforme a figura 1.3. Nesta o autor, cito [6], observa que a construção pode ser realizada para qualquer valor $a > 0$, o qual será escolhido convenientemente, baseado na construção e de modo que $\sum_j \alpha_j = 2\pi$.

Feito isso, concatena-se todos estes quadriláteros, de forma que os vértices v'_j e v''_{j+1} se sobreponham, bem como as arestas $[O, v'_j]$ e $[O, v''_{j+1}]$, a fim de obter o polígono buscado.

É importante destacar nesta construção a perpendicularidade entre os segmentos de geodésica $[O, v'_j]$ e $[v_j, v'_j]$: O segmento $[v_j, v'_j]$, ao ser concatenado com o segmento $[v_{j+1}, v'_{j+1}]$, dará lugar a uma das arestas do polígono. Esta, por sua vez, é ortogonal ao segmento de geodésica $[O, v'_j] = [O, v''_{j+1}]$, que determina o raio da circunferência inscrita.

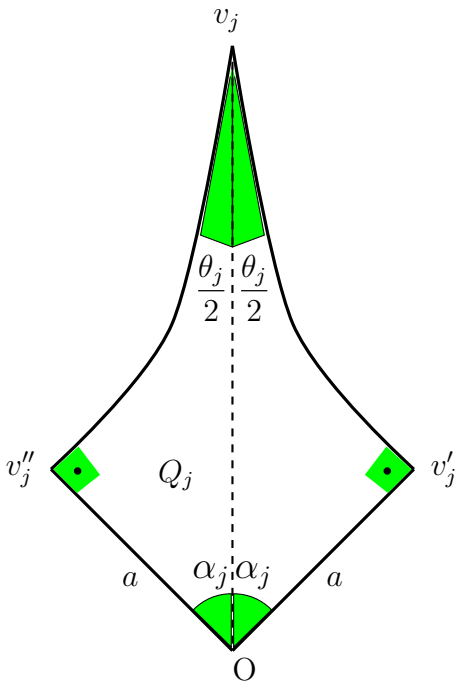


Figura 1.3: Representação de um quadrilátero com dois ângulos retos, um medindo α_j e outro medindo θ_j.

Em particular, quando o polígono P é regular, cada apótema é o segmento de reta determinado pelo ponto médio de uma de suas arestas, à qual é perpendicular, e o seu incentro.

Desconsiderando as propriedades métricas de uma tesselação, obtemos um grafo. A Tesselação Dual de uma tesselação dada é aquela obtida canonicamente pelo grafo dual do grafo subjacente a esta. Mais precisamente, fixada uma tesselação cujas faces possuam

incentro, a tesselação dual a esta é a tesselação construída da seguinte maneira: Cada incentro da tesselação fixada passa a ser um vértice da tesselação dual, enquanto que cada segmento de geodésica que conecta os incentros de dois polígonos adjacentes determina uma aresta. Notando que, fixado um vértice v da tesselação original que possui valência q, em seu entorno existem exatamente q incentros que, ao serem conectados pelas arestas da tesselação dual, determinam um q-gon. Reciprocamente, fixada uma face da tesselação original, que sem perda de generalidade podemos supor um p-gon, nota-se que do seu incentro, que é um vértice da tesselação dual, partem p arestas, também da tesselação dual, cada uma cortando perpendicularmente exatamente uma aresta deste polígono. Isto faz com que tal vértice da tesselação dual tenha valência p.

Em particular, a tesselação dual da tesselação regular $\{p, q\}$ é a tesselação regular $\{q, p\}$.

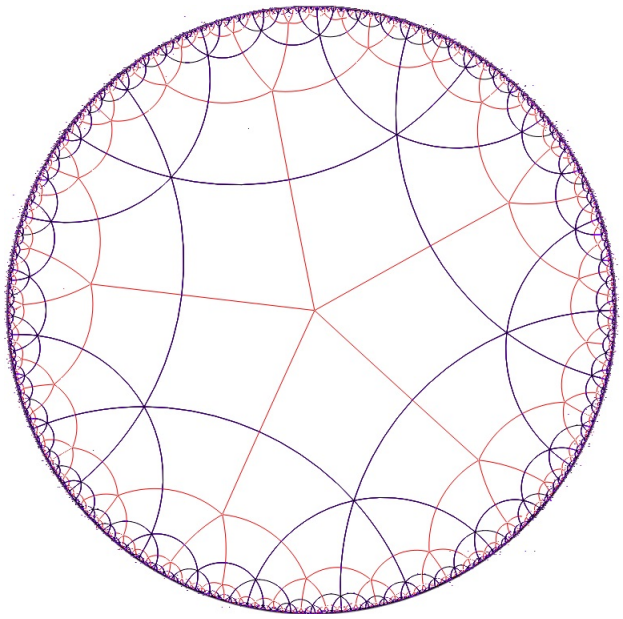


Figura 1.4: Tesselações do disco de Poincaré. Em preto: Tesselação $\{5, 6\}$. Em vermelho: Tesselação $\{6, 5\}$, dual da tesselação $\{5, 6\}$.

1.5.1 Tesselações do Plano Hiperbólico

Em se tratando de tesselações regulares do plano euclidiano, dado um vértice v qualquer de uma dada tesselação $\{p, q\}$, a medida do ângulo interno de cada polígono é, obrigatoriamente, $\frac{2\pi}{q}$. Isto garante que, ao se decompor canonicamente tal polígono em p triângulos, os ângulos internos deste devem ser $\frac{\pi}{q}$, $\frac{\pi}{q}$ e $\frac{2\pi}{p}$, de onde segue que $\frac{2\pi}{p} + \frac{2\pi}{q} = \pi$, ou seja, $(p-2)(q-2) = 4$. Assim, os únicos candidatos à tesselação regular, na geometria euclidiana, são a $\{3, 6\}$, $\{6, 3\}$ e $\{4, 4\}$. De fato existem tesselações regulares com estes parâmetros, a saber, aquela por triângulos, hexágonos e por quadrados, respectivamente.

A curvatura negativa de um espaço com métrica hiperbólica possibilita a existência de uma infinidade de tesselações. Em particular, enquanto o plano euclidiano admite apenas três tesselações regulares, o plano hiperbólico admite uma infinidade de tesselações regulares, considerando a sua geometria. Obviamente, a existência de uma tesselação regular $\{p, q\}$ do plano hiperbólico faz exigência de uma relação entre os parâmetros p e q.

Teorema 1.5.3. *Sejam p, q inteiros maiores do que 2. Existe uma tesselação $\{p, q\}$ de $\mathbb{D}$ se, e somente se, $\frac{1}{p} + \frac{1}{q} < \frac{1}{2}$.*

Assim, existe uma tesselação de $\mathbb{D}$ se, e só se, $(p-2)(q-2) - 4 > 0$. Esta inequação admite infinitas soluções inteiras. Conforme realizado em [22] e [51], as tesselações regulares nos serão úteis, pois construiremos superfícies hiperbólicas a partir de um polígono de uma tesselação regular de $\mathbb{D}$, mediante uma identificação de arestas e um quociente do disco de Poincaré por um grupo que age propriamente descontinuamente neste.

1.5.2 Superfícies Hiperbólicas

O teorema de Killing-Hopf trata, em sua forma original, de variedades Riemannianas. Trazemos abaixo a sua adaptação para o caso em que utilizamos aqui, por meio de uma mera restrição. Mais detalhes deste podem ser encontrados em [53, 4].

Teorema 1.5.4. *(Killing-Hopf Geral, [53]) Qualquer superfície de curvatura constante, completa e conexa, é um quociente ou de um espaço euclidiano, ou hiperbólico ou esférico, por um grupo de isometrias, que nele atua propriamente descontinuamente e livre de pontos fixos.*

Vamos tratar aqui de construir superfícies hiperbólicas por meio do quociente de $\mathbb{D}$ por grupos Fuchsianos específicos. Um ingrediente relevante para esta construção é a noção de emparelhamento de lados: Dado um polígono de n lados $\mathbb{P}$, contido no interior de $\mathbb{D}$, juntamente com uma orientação de suas arestas, e uma indexação de seus vértices, digamos $v_1, \cdots, v_n$, e de seus lados, $s_1, \cdots, s_n$, um emparelhamento entre os lados s_k e s_l é uma aplicação $\gamma_{k,l} \in M\ddot{o}b(\mathbb{D})$, tal que $\gamma_{k,l}(s_k) = s_l$, que preserva a orientação estabelecida.

Dado um par $\binom{v}{s}$, onde s é uma aresta do polígono hiperbólico $\mathbb{P}$ e v é um vértice de s, denotamos por $\star\binom{v}{s} = \binom{v}{\star s}$ o par composto pelo mesmo vértice v, e com a aresta $\star s$, a qual é a aresta distinta de s que contém v. A figura 1.5 exemplifica a aplicação do operador $\star$.

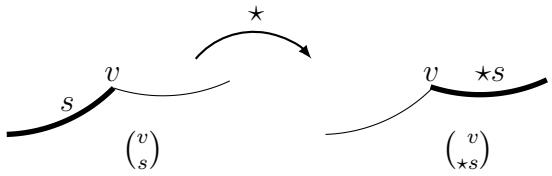


Figura 1.5: Ilustração da aplicação $\star(\quad)$

Para cada aresta s_j do polígono $\mathbb{P}$, escolha uma aplicação de emparelhamento de arestas γ_j e considere a seguinte construção: Fixado um par $\binom{v_0}{s_0}$, defina $s_1 = \gamma_1(s_0)$ e $v_1 = \gamma_1(v_0)$, onde v_i é um vértice e s_j é uma aresta de $\mathbb{P}$. Agora, defina indutivamente $s_{k+1} = \gamma_{k+1}(\star s_k)$ e $v_{k+1} = \gamma_{k+1}(v_k)$. Como a quantidade de vértices de $\mathbb{P}$ é finita, obrigatoriamente para algum $j > 0$ deve ocorrer que $\binom{v_j}{\star s_j} = \binom{v_0}{s_0}$. Se j_0 é o menor inteiro positivo com esta propriedade, chamamos de Ciclo de Vértices à sequência $\varepsilon = v_0 \to v_1 \to \cdots \to v_{j_0-1}$ e de Transformação de Ciclo Elíptico à transformação $\gamma_\varepsilon = \gamma_{j_0}\gamma_{j_0-1}\cdots\gamma_1$. Eventualmente existe mais de um ciclo de vértices de $\mathbb{P}$, porém, cada vértice pertence a um único ciclo. A Soma dos Ângulos do ciclo de vértices ε, é a soma dos ângulos internos de $\mathbb{P}$, em cada um dos vértices v de ε, ou seja, $Sum(\varepsilon) = \sum_{v_j \in \varepsilon} \angle(v_j)$. Dizemos que um ciclo de vértices satisfaz a Condição de Ciclo Elíptico se existe um número inteiro $m > 0$, tal que $m\ Sum(\varepsilon) = 2\pi$. Um ciclo elíptico ε é dito Acidental se $Sum(\varepsilon) = 2\pi$.

A figura 1.6 ilustra um polígono de oito lados com emparelhamento de lados opostos. O ciclo de vértices relativo à este emparelhamento de arestas é $v_1 \to v_6 \to v_3 \to v_8 \to v_5 \to v_2 \to v_7 \to v_4$, enquanto que a transformação de ciclo elíptico é $\gamma_4^{-1}\gamma_3^{-1}\gamma_2^{-1}\gamma_1^{-1}\gamma_4\gamma_3\gamma_2\gamma_1$.

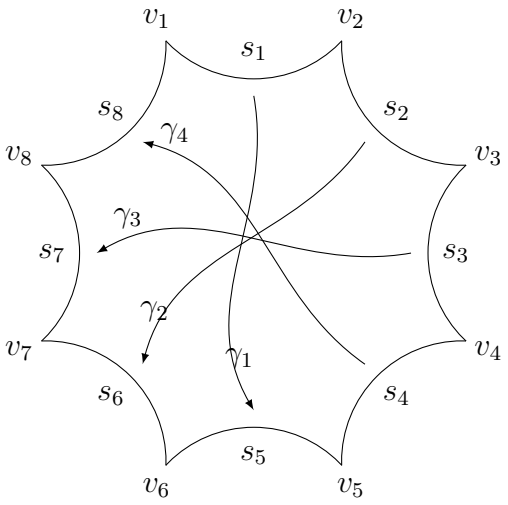


Figura 1.6: Polígono de 8 lados, com lados opostos emparelhados.

Este polígono pode, por exemplo, ser obtido com a tesselação regular $\{8,3\}$ ou com a $\{8,8\}$. Em ambos os casos os ciclos elípticos satisfazem a condição de ciclo elíptico, porém apenas no segundo este é acidental. O esquema que ilustra o ciclo de vértices é o seguinte:

$$\binom{v_1}{s_1} \xrightarrow{\gamma_1} \binom{v_6}{s_5} \xrightarrow{\star} \binom{v_6}{s_6} \xrightarrow{\gamma_2} \binom{v_3}{s_2} \xrightarrow{\star} \binom{v_3}{s_3} \xrightarrow{\gamma_3} \binom{v_8}{s_7} \xrightarrow{\star} \binom{v_8}{s_8} \xrightarrow{\gamma_4} \binom{v_5}{s_4} \xrightarrow{\star} \binom{v_5}{s_5}$$
$$\binom{v_5}{s_5} \xrightarrow{\gamma_1^{-1}} \binom{v_2}{s_1} \xrightarrow{\star} \binom{v_2}{s_2} \xrightarrow{\gamma_2^{-1}} \binom{v_7}{s_6} \xrightarrow{\star} \binom{v_7}{s_7} \xrightarrow{\gamma_3^{-1}} \binom{v_4}{s_3} \xrightarrow{\star} \binom{v_4}{s_4} \xrightarrow{\gamma_4^{-1}} \binom{v_1}{s_8} \xrightarrow{\star} \binom{v_1}{s_1}.$$

Teorema 1.5.5 (Poincaré, [39, 6])**.** *Seja $\mathbb{P}$ um polígono hiperbólico convexo que possui uma quantidade finita de lados, completamente contido no interior de $\mathbb{D}$. Suponha que $\mathbb{P}$ está equipado com um conjunto de transformações de emparelhamento de lados $\mathcal{G}$, cujos (todos os) ciclos elípticos são $\varepsilon_1, \cdots, \varepsilon_t$, e de modo que nenhum lado de $\mathbb{P}$ está emparelhado consigo mesmo. Suponha, adicionalmente, que cada ciclo elíptico ε_j satisfaz a condição de ciclo elíptico, com $m_j Sum(\varepsilon_j) = 2\pi$. Nestas condições, tem-se:*

i. $\Gamma = \langle \mathcal{G} \rangle$ *é um grupo Fuchsiano;*

ii. O polígono $\mathbb{P}$ é um domínio fundamental para Γ;

iii. O grupo Γ pode ser descrito em termos de geradores e relações. Para cada ciclo elíptico ε_j, escolha uma transformação de ciclo elíptico $\gamma_j = \gamma_{\varepsilon_j}$. O grupo Γ pode ser gerado pelos elementos γ_j e com relações $\gamma_j^{m_j} = Id$ como segue:

$$\Gamma = \langle \gamma_j \in \mathcal{G} | \gamma_j^{m_j} = Id, j = 1, \cdots, t \rangle.$$

Observação 1.5.6. A transformação de ciclo elíptico γ_j empregada no teorema 1.5.5 depende do vértice e da aresta na qual o processo de confecção desta se inicia. Embora distintas escolhas de vértices e/ou arestas iniciais levam em aplicações eventualmente distintas, estas diferem apenas por uma permutação cíclica na ordem de composição. Para o presente teorema, esta característica é irrelevante.

Considere a tesselação do plano euclidiano dado por quadrados de lado unitário. Esta tesselação nada mais é do que um recobrimento do plano por regiões fundamentais do grupo das translações inteiras do plano. É fato que este grupo atua no plano de maneira propriamente descontínua. O quociente do plano euclidiano por este grupo acaba por identificar todos os pontos da órbita de cada ponto. Em particular, cada par de arestas opostas de um quadrado qualquer estão identificadas mediante este argumento. Tomando tal quadrado e metaforicamente colando todos os pontos mutuamente identificados, percebemos que a superfície resultante deste quociente é o toro de gênus 1. A figura 1.7 ilustra esta situação.

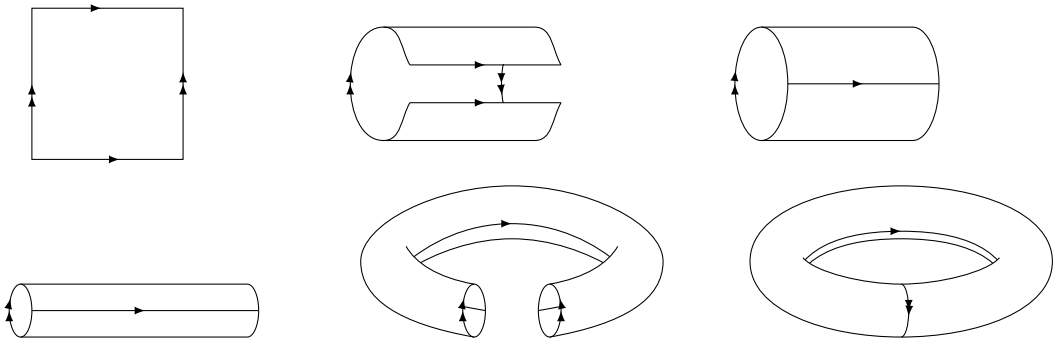


Figura 1.7: Ilustração de um quadrado que é região fundamental do grupo de translações inteiras dando lugar ao 1-toro, mediante a "colagem"dos lados opostos identificados. Intuitivamente, este é o processo que ocorre no quociente do plano euclidiano, pelo grupo das translações inteiras.

Com um processo similar, a identificação de lados opostos do polígono de oito lados fornece, segundo o teorema de Poincaré, 1.5.5, um grupo Fuchsiano Γ. O quociente de $\mathbb{D}$ por tal grupo, determina uma "colagem" de arestas e vértices identificados, segundo o ciclo de vértices descrito na figura 1.6. Este resulta no 2-toro, conforme indicado na figura 1.8.

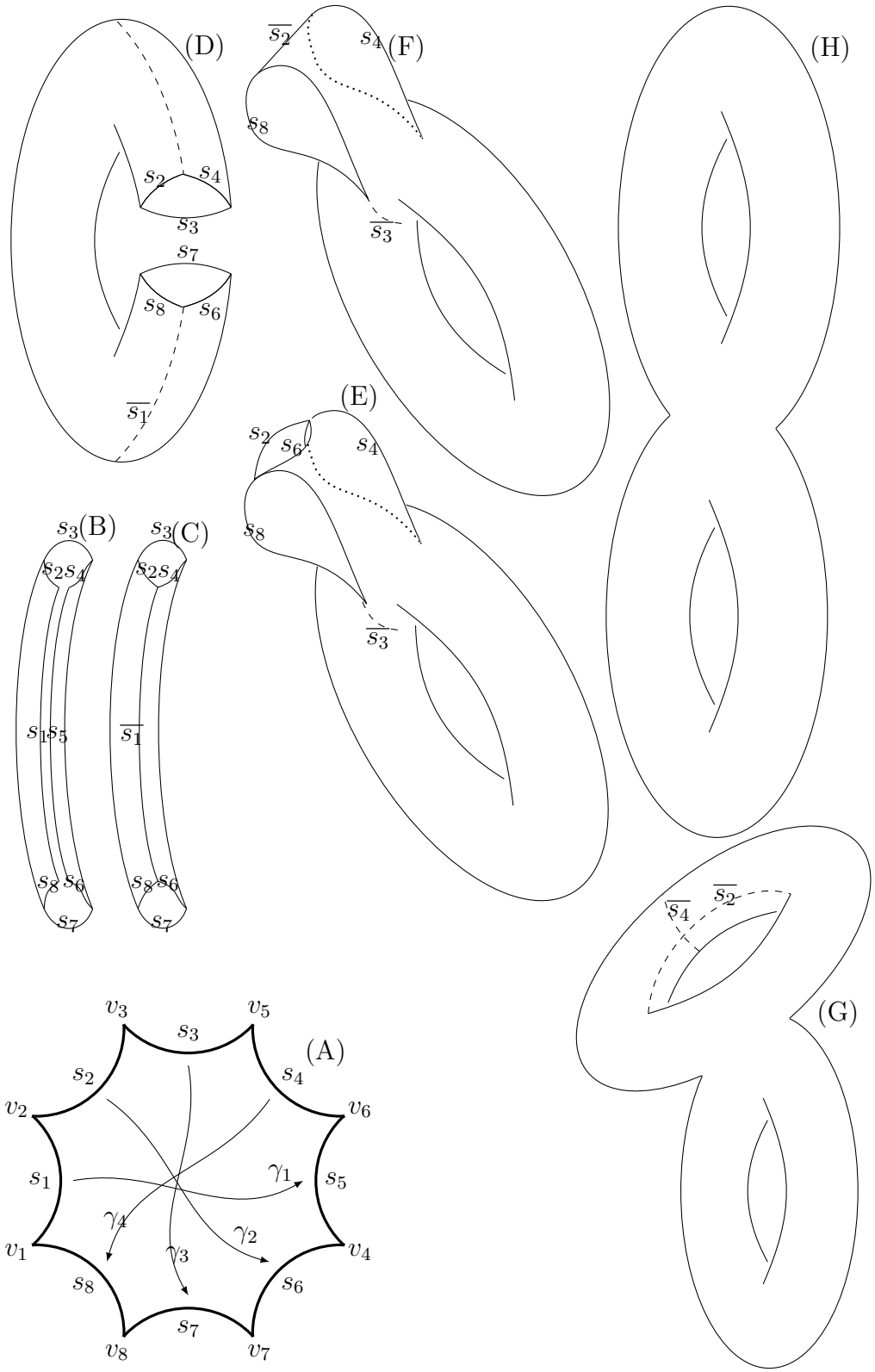


Figura 1.8: Ilustração da construção do 2-toro desde um 8-gon, com lados opostos pareados. (figura baseada em similar de [49]).

Considere um $4g$-gon regular $\mathbb{P}$, munido de um emparelhamento de lados opostos, implementado de forma que se tenha somente um ciclo elíptico. Se este ciclo elíptico é acidental, a superfície $\mathbb{D}/\Gamma$, onde Γ é o grupo Fuchsiano associado à identificação de lados dada, é o $g-$toro. Se $g > 1$, a superfície conta com uma métrica hiperbólica, de forma que a projeção $\pi : \mathbb{D} \to \mathbb{D}/\Gamma$ é uma isometria local, o que força $\mathbb{D}/\Gamma$ ser uma superfície hiperbólica. A existência de um único ciclo de vértices ε força que se θ é a medida de cada ângulo interno de $\mathbb{P}$, então $Sum(\varepsilon) = 4g\theta$. Para que o ciclo de vértices seja acidental, requer-se que $\theta = \frac{2\pi}{4g}$. Este polígono pode ser obtido em uma face da tesselação $\{4g, 4g\}$. De agora em diante, a menos de menção contrária, estaremos considerando superfícies hiperbólicas assim obtidas.

A característica de Euler de uma superfície $\mathbb{M}$ é obtida através de uma triangulação desta. Se V, E e F são, respectivamente, o número de vértices, arestas e faces desta triangulação, então a característica de Euler de $\mathbb{M}$ é $\chi(\mathbb{M}) = V - E + F$. Obviamente não é nada prático obter triangulações e realizar sua contagem sobre uma superfície. Para contornar esta situação, lançamos mão do seguinte resultado: Se $\mathbb{M}$ é uma superfície orientável, compacta e conexa, de gênus g, então $\chi(\mathbb{M}) = 2(1-g)$. Portanto, se $\mathbb{M}$ é o g-toro obtido do $4g$-gon, da tesselação regular $\{4g, 4g\}$ de $\mathbb{D}$, então $\chi(\mathbb{M}) = 2(1-g)$.

1.5.3 Tesselações de Superfícies Hiperbólicas

Tesselar uma superfície $\mathbb{M}$ consiste em obter uma partição da mesma em polígonos regulares, de interior disjunto e sem sobreposição, $\mathbb{P}_1^{s_1}, \cdots, \mathbb{P}_{\alpha_1}^{p_1}, \cdots, \mathbb{P}_1^{p_r}, \cdots, \mathbb{P}_{\alpha_r}^{p_r}$, onde $\mathbb{P}_\alpha^{p_j}$ é um p_j-gon e cada par de p_j-gons são congruentes, independente da escolha de $j = 1, \cdots, r$. Numa tesselação, quando dois polígonos se intersectam, o fazem ao longo de uma aresta ou de um vértice. A tesselação de uma superfície $\mathbb{M}$ é dita semirregular se todos os vértices tem o mesmo tipo, enquanto que uma tesselação semirregular é dita regular se $p_1 = p_2 = \cdots = p_r$.

Tesselações Regulares de Superfícies Hiperbólicas

Suponha que uma tesselação $\{p, q\}$ de $\mathbb{D}$ é tal que algumas de suas faces, que são p-gons $\mathbb{P}$, tesselam o g-toro $\mathbb{M}$. Se $\mu(\mathbb{M})$ e $\mu(\mathbb{P})$ são, respectivamente, as áreas de $\mathbb{M}$ e $\mathbb{P}$ e F é o número de faces desta tesselação em $\mathbb{M}$, então:

$$\mu(\mathbb{M}) = F\mu(\mathbb{P}). \tag{1.10}$$

Para fins combinatórios, seja V o número de vértices e E o número de arestas desta tesselação de $\mathbb{M}$. Por um instante, considere as meia-arestas da tesselação, que são os segmentos de geodésica obtidos pela metade de uma aresta, determinado pelo seu ponto médio e por um dos seus vértices. Se a quantidade de meias-arestas é E', tem-se $E' = 2E$. Como de cada vértice emanam q meias-arestas, temos $qV = E'$, isto é, $qV = 2E$. Similarmente, se os polígonos fossem desacoplados, cada vértice daria lugar a q novos vértices. Essa nova quantidade de vértices seria igual a pF, de onde, $qV = pF$. Juntando estas relações, temos:

$$qV = 2E = pF. \tag{1.11}$$

Observação 1.5.7. i. O incentro de p-gon regular determina a decomposição deste em p triângulos congruentes, cada um com ângulos internos $\frac{\pi}{q}$, $\frac{\pi}{q}$ e $\frac{2\pi}{p}$. Segundo o teorema de Gauss-Bonnet para triângulos hiperbólicos, cito teorema 1.4.9, a área de cada um destes triângulos é igual a $\frac{pq-2p-2q}{pq}\pi$. Portanto, a área do p-gon regular, cujos ângulos internos medem $\frac{2\pi}{q}$ é dada por $\mu(\mathbb{P}) = \frac{pq-2p-2q}{q}\pi$;

ii. Se $g \geq 2$ e $\{p, q\}$ é uma tesselação regular sobre o g-toro $\mathbb{M}$, esta consta de $F = \frac{4(g-1)q}{pq-2p-2q}$ faces, $E = \frac{2(g-1)pq}{pq-2p-2q}$ arestas e $V = \frac{4(g-1)p}{pq-2p-2q}$ vértices. Segue então que:

$$V - E + F = \frac{4(g-1)p}{pq-2p-2q} - \frac{2(g-1)pq}{pq-2p-2q} + \frac{4(g-1)q}{pq-2p-2q} = 2(1-g);$$

iii. Se $\{p, q\}$ é uma tesselação regular, seja do plano hiperbólico ou de uma superfície hiperbólica, cujo comprimento de aresta é l, também é válida a relação:

$$l_{p,q} = \operatorname{arccosh}\left[\frac{\cos^2\left(\frac{\pi}{q}\right) + \cos\left(\frac{2\pi}{p}\right)}{\operatorname{sen}^2\left(\frac{\pi}{q}\right)}\right].$$

Esta decorre da aplicação direta da 2ª lei dos cossenos para triângulos hiperbólicos no triângulo determinado por dois vértices adjacentes, juntamente com o incentro de um

dado polígono qualquer desta tesselação.

Proposição 1.5.8. Seja $\mathbb{M}$ uma superfície compacta, conexa e orientável, de gênus $g \geq 2$, e p, q, V, E, F inteiros positivos, tais que $\mu(\mathbb{M}) = F\mu(\mathbb{P})$, onde $\mathbb{P}$ é um p-gon de ângulos internos medindo $\frac{2\pi}{q}$. Notando que $F = \frac{4q(g-1)}{pq-2p-2q}$, se $pF = 2E = qV$, então $V - E + F = \chi(\mathbb{M})$.

Embora sejam necessárias para a existência de uma tesselação regular $\{p, q\}$ de uma superfície compacta, conexa e orientável $\mathbb{M}$, estas relações não são, por si só, suficientes para tal. O que nos permite utilizá-las, a fim de estudar a existência de determinadas tesselações regulares de uma superfície, está contido no teorema 1.5.9, o qual foi obtido em [28].

Teorema 1.5.9 ([28])**.** *Seja $\mathbb{M}$ uma superfície compacta, conexa e orientável, e p, q, V, E, F inteiros positivos, tais que $V - E + F = \chi(\mathbb{M})$ e $pF = 2E = qV$. São válidas as proposições:*

i. (Existência:) Existe um $\{p, q\}$-padrão em $\mathbb{M}$, com F faces, E arestas e V vértices, cada um com valência q, exceto quando $\mathbb{M}$ é o plano projetivo, $p = q = E = 3$ e $V = F = 2$;

ii. (Geometrização) Um $\{p, q\}$-padrão em $\mathbb{M}$ pode ser realizado geometricamente;

iii. (Classificação) Um $\{p, q\}$-padrão na esfera ou no plano projetivo é único. Para todas as outras superfícies $\mathbb{M}$, os $\{p, q\}$-padrão em $\mathbb{M}$, são classificados por classes de conjugação de subgrupos isomorfos ao grupo fundamental de $\mathbb{M}$ nos grupos de Schwarz estendidos $(p, q, 2)$-triângulo.

Os dois primeiros itens deste teorema são os que de fato nos interessam. Estes garantem que, satisfeitas as condições 1.10 e 1.11, então existe uma tesselação regular $\{p, q\}$ de $\mathbb{M}$. A condição restante da hipótese do teorema é automaticamente satisfeita nesta ocasião.

Dada uma tesselação regular $\{p, q\}$ do plano hiperbólico, o seu comprimento de aresta pode ser calculado através da trigonometria para triângulos hiperbólicos. De início, a aplicação das relações 1.5 e 1.6 sobre uma face qualquer da tesselação fornece:

Proposição 1.5.10. Dada a tesselação regular $\{p, q\}$ do plano hiperbólico, onde $l_{p,q}$ é o comprimento de aresta, $a_{p,q}$ e $r_{p,q}$ são comprimentos dos raios das circunferências inscrita e circunscrita a uma de suas faces, respectivamente, são válidas as seguintes relações:

$$l_{p,q} = 2\,\text{arccosh}\left[\cos\left(\frac{\pi}{p}\right)\text{cossec}\left(\frac{\pi}{q}\right)\right]; \tag{1.12}$$

$$a_{p,q} = \text{arccosh}\left[\text{cossec}\left(\frac{\pi}{p}\right)\cos\left(\frac{\pi}{q}\right)\right]; \tag{1.13}$$

$$r_{p,q} = \text{arccosh}\left[\text{cotg}\left(\frac{\pi}{p}\right)\text{cotg}\left(\frac{\pi}{q}\right)\right]. \tag{1.14}$$

Observação 1.5.11. Alternativamente, satisfeitas as hipóteses do teorema 1.5.10, também é válida a relação:

$$l_{p,q} = \text{arccosh}\left[\frac{\cos^2\left(\frac{\pi}{q}\right) + \cos\left(\frac{2\pi}{p}\right)}{\text{sen}^2\left(\frac{\pi}{q}\right)}\right].$$

Corolário 1.5.12. Se $\mathbb{M}$ é um g-toro, $g \geq 2$, que é obtido a partir de um polígono da tesselação $\{4g, 4g\}$ por meio de emparelhamento de arestas opostas, o menor ciclo de homologia não trivial sobre este tem comprimento $d_{\mathbb{M}} = 2\,\text{arccosh}\left[\text{cotg}\left(\frac{\pi}{4g}\right)\right]$.

Observação 1.5.13.

i. O comprimento de aresta de uma tesselação regular $\{p, p\}$ do plano hiperbólico coincide com o diâmetro da circunferência inscrita a um de seus polígonos;

ii. A área de $\mathbb{M}$ é dada por $\mu(\mathbb{M}) = 4\pi(g-1)$.

Tesselações Semirregulares de Superfícies Hiperbólicas Derivadas de Regulares

Os processos de derivação de tesselações regulares descritos aqui, embora estarem sendo considerados relativamente a uma tesselação regular de uma superfície $\mathbb{M}$ que cumpre as condições acima listadas, podem ser perfeitamente desenvolvidos sobre uma tesselação regular do plano hiperbólico. Estes processos de derivação são intrínsecos das tesselações e não dependem do ambiente onde elas estão inseridas.

Dada uma tesselação regular $\{p, q\}$ de uma superfície $\mathbb{M}$, considere a tesselação obtida conectando-se os pontos médios de todos os pares de arestas adjacentes, conforme ilustrado na figura 1.9. Este processo é conhecido como Derivação por Ponto Médio.

Sejam n_f, n_e e n_v as quantidades de faces, arestas e vértices, respectivamente, componentes da tesselação original, enquanto que N_f, N_e e N_v são as quantidades de faces, arestas

e vértices, respectivamente, componentes da tesselação derivada. Assim sendo, ao notar que internamente a cada um dos n_f p-gons da tesselação original se constrói um novo p-gon e que centralizado em cada um dos n_v vértices da tesselação original se constrói um q-gon, segue que $N_f = n_f + n_v$. Através de um raciocínio similar, cada aresta da tesselação derivada, neste caso, é uma arestas de um único q-gon ou, alternativamente, é aresta de um único p-gon da tesselação derivada. Disto, $N_e = qn_v = pn_f$. Finalmente, cada vértice da tesselação derivada está situado sobre uma única aresta da tesselação original. Segue disto que $N_v = n_e = \frac{pn_f}{2}$.

O interesse em determinar as quantidades de vértices, arestas e faces da tesselação derivada reside em estabelecer, mais adiante, parâmetros de códigos quânticos corretores de erros que estas vão fornecer. Faremos, portanto, este trabalho com mais duas construções.

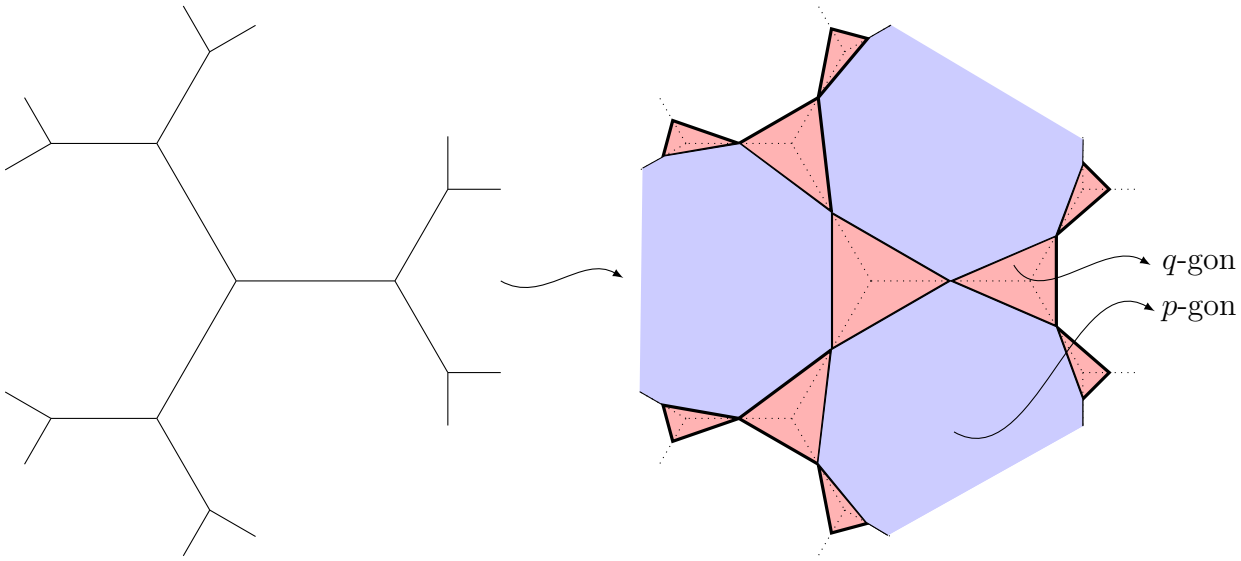


Figura 1.9: A tesselação derivada por ponto médio de $\{p, q\}$ é a tesselação $[p, q, p, q]$.

Observação 1.5.14. Se L denota o comprimento de aresta desta tesselação derivada e a é o comprimento do apótema de um polígono da tesselação original, isto é, a é o comprimento do raio da circunferência inscrita a tal polígono, então $L = 2\,\text{arcsenh}\left[\text{senh}\,(a)\,\text{sen}\left(\frac{\pi}{p}\right)\right]$. De fato, obtém-se aplicando a relação 1.3 no triângulo retângulo cujo cateto oposto ao ângulo que mede $\frac{\pi}{p}$ tem comprimento igual a $\frac{L}{2}$ e cujo cateto que é oposto ao ângulo que mede $\frac{\pi}{2q}$ tem o mesmo comprimento do apótema a de uma face da tesselação original. Por questões de organização do texto, o apótema agora citado está calculado mais adiante.

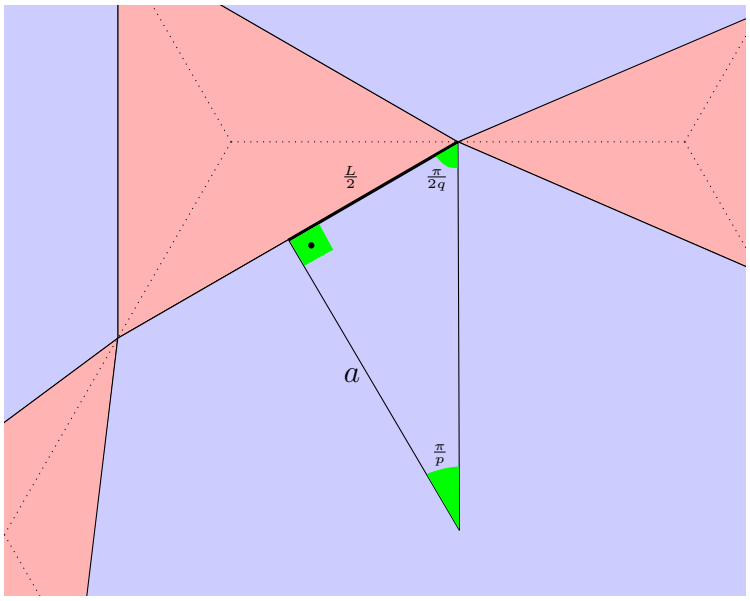


Figura 1.10: Triângulo que fornece o comprimento de aresta da tesselação semirregular $[p, q, p, q]$ mediante a aplicação direta da relação 1.3.

Dada a tesselação regular $\{p, q\}$, podemos "cortar" a região próxima ao vértice de cada p-gon, de forma que este dê lugar a um $2p$-gon regular. Com este processo, que é conhecido por Derivação por Clipping, surgem ao redor de cada um dos n_v vértices da tesselação original um q-gon e, como dissemos, internamente a cada um dos n_f p-gons da tesselação original, um $2p$-gon. Tem-se então, $N_f = n_f + n_v$. Já o conjunto de arestas da tesselação derivada é constituído por n_e arestas, que são segmentos de aresta da tesselação original, juntamente com qn_v arestas provenientes dos novos q-gons centralizados em vértices da tesselação original. Tem-se, portanto, $N_e = n_e + qn_v = \frac{3}{2}pn_f$. Observado que cada uma das n_e arestas da tesselação original comporta um par de vértices da derivada, ou mesmo que cada vértice da tesselação derivada é um vértice de algum dos n_v q-gons, tem-se $N_v = 2n_e = qn_v = pn_f$.

A tesselação derivada por clipping de $\{p, q\}$ é a tesselação $[2p, 2p, q]$. Vide figura 1.11.

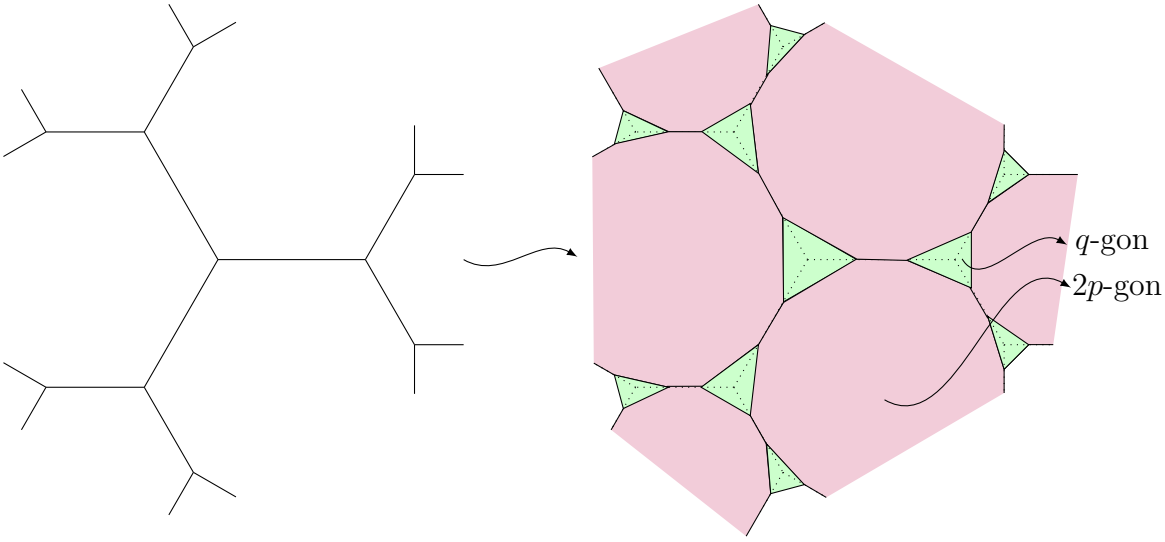


Figura 1.11: A tesselação derivada por clipping de $\{p, q\}$ é a tesselação semirregular $[2p, 2p, q]$.

Observação 1.5.15. Se L denota o comprimento de aresta desta tesselação derivada e a é o comprimento do apótema da tesselação original, então $L = 2\,\text{arctgh}\left[tg\left(\frac{\pi}{2p}\right)\text{senh}\,(a)\right]$. A figura 1.12 ilustra o triângulo que é tomado como base para estes cálculos.

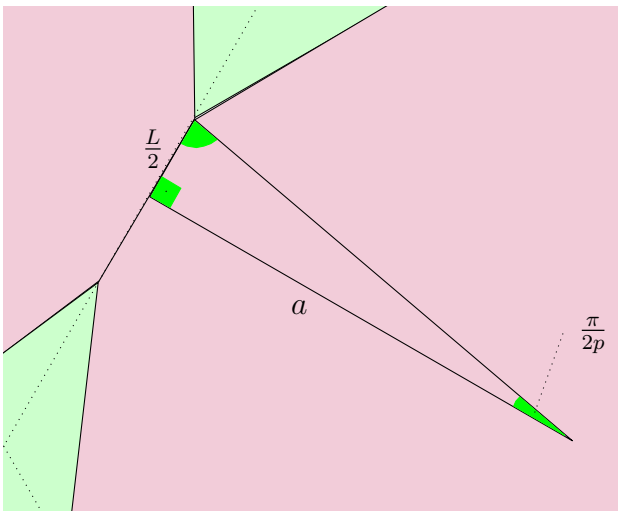


Figura 1.12: Triângulo que fornece o comprimento de aresta da tesselação semirregular $[2p, 2p, q]$ mediante a aplicação direta da relação 1.2.

Similarmente podemos derivar da tesselação $\{p, q\}$ de $\mathbb{M}$ a tesselação semirregular $[2p, 2q, 4]$, utilizando o processo de Derivação por Incentro, o qual consiste inicialmente em traçar os raios das circunferências inscritas e circunscritas à cada face, respectivamente. Este processo decompõe cada face em $2p$ triângulos retângulos. Traçando segmentos de geodésica entre o

incentro de todos os pares de triângulos com aresta em comum, e descartando-se as arestas da tesselação original, bem como a destes triângulos, obtém-se a tesselação semirregular citada.

Denotando por n_f, n_e e n_v as quantidades de faces, arestas e vértices da tesselação original, respectivamente, e por N_f, N_e e N_v as quantidades de faces, arestas e vértices da tesselação derivada, respectivamente, tem-se $N_f = n_f + n_v + n_e$, visto que o processo constrói um $2p$-gon centralizado em um dos n_f p-gons da tesselação original, um 4-gon centralizado no ponto médio de cada uma das n_e arestas da tesselação original e um $2q$-gon centralizado em cada um dos n_v vértices da tesselação original. Tem-se também $N_e = 3pn_f$, visto que existem $2pn_f$ arestas de $2p$-gons, juntamente com duas arestas transversais a cada uma das n_e arestas da tesselação original, as quais compõem os 4-gons. Para estabelecer a relação, basta lembrar que $2n_e = pn_f$. Finalmente, cada vértice da tesselação derivada está sobre exatamente um dos n_f $2p$-gons, de onde segue que $N_v = 2pn_f$. Vide figura 1.13.

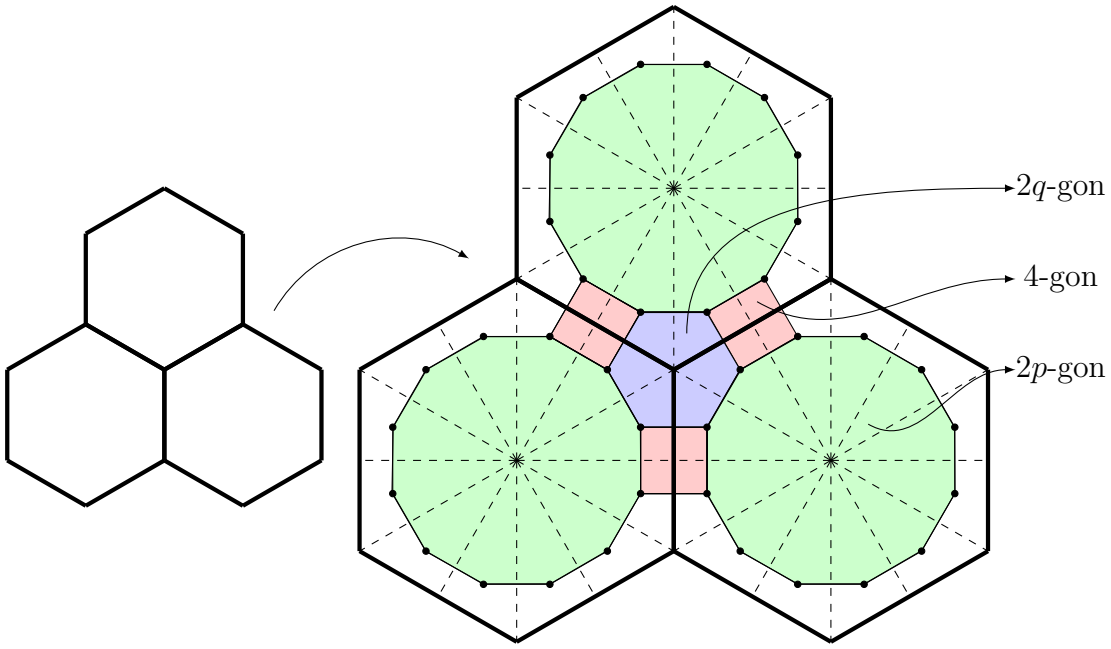


Figura 1.13: A tesselação derivada por incentro de $\{p, q\}$ é a tesselação semirregular $[2p, 2q, 4]$.

Observação 1.5.16. Se L denota a medida da aresta desta tesselação derivada, então:

$$L = 2\,\mathrm{arctgh}\left[\sqrt{\frac{\cos^2\left(\frac{\pi}{p}\right) + \cos^2\left(\frac{\pi}{q}\right) - 1}{2\left(1+\cos\left(\frac{\pi}{p}\right)\right)\left(1+\cos\left(\frac{\pi}{q}\right)\right)}}\right].$$

Esta relação é obtida quando aplicado o lema 1.4.8 no triângulo que fornece o incentro a ser utilizado no processo de construção da tesselação derivada. O raio da circunferência inscrita em tal triângulo tem metade do comprimento de aresta da tesselação derivada.

Observação 1.5.17. A tabela abaixo fornece as quantidades N_f, N_e e N_v em função de p e q, partindo do fato de que $pn_f = 2n_e = qn_v$ e que $nf = \dfrac{4q(g-1)}{pq-2p-2q}$.

Tesselação	N_f	N_e	N_v
$[2p, 2p, q]$	$\dfrac{4(p+q)(g-1)}{pq-2p-2q}$	$\dfrac{6pq(g-1)}{pq-2p-2q}$	$\dfrac{4pq(g-1)}{pq-2p-2q}$
$[2p, 2q, 4]$	$\dfrac{2(pq+2p+2q)(g-1)}{pq-2p-2q}$	$\dfrac{12pq(g-1)}{pq-2p-2q}$	$\dfrac{8pq(g-1)}{pq-2p-2q}$
$[p, q, p, q]$	$\dfrac{4(p+q)(g-1)}{pq-2p-2q}$	$\dfrac{4pq(g-1)}{pq-2p-2q}$	$\dfrac{2pq(g-1)}{pq-2p-2q}$

1.6 Tesselações Semirregulares em Superfícies Orientáveis

Embora os casos contemplados na seção 1.5.3 sejam interessantes para o nosso estudo de códigos quânticos corretores de erros, tanto topológicos quanto coloridos como veremos mais adiante, não são suficientes para o escopo deste texto e ainda contam com a limitação de dependerem da posse de uma tesselação regular. Porém, o teorema 1.6.1 nos fornece uma infinidade de tesselações semirregulares do g-toro, que são suficientemente independentes de qualquer tesselação regular para o nosso estudo. Como antes, $\mathbb{M}$ denotará uma superfície conexa, compacta e orientável.

Teorema 1.6.1 ([29, 30])**.** *Seja $\mathbb{M}$ uma superfície, $p_1, \cdots p_t$, R, E, $V_1, \cdots, V_t$ inteiros positivos, tais que $2E = tR$, $2p_iV_i = R$ e $R - E + \sum_{i=1}^{t} V_i = \chi(\mathbb{M})$. Nestas condições, existe uma tesselação de $\mathbb{M}$ constituída por R t-gons, E arestas, e $\sum_{i=1}^{t} V_i$ vértices, dos quais V_i destes possuem valência $2p_i$, de forma que cada t-gon tem vértices de valência $2p_1, \cdots, 2p_t$, nesta ordem, a menos de uma permutação cíclica.*

Tendo em vista que uma tesselação geométrica de uma superfície $\mathbb{M}$ é toda aquela obtida através de um polígono $\mathbb{P}$, que é um domínio fundamental do grupo de reflexões através de

suas arestas, consideremos a proposição a seguir. Esta nos garante que, a menos de uma equivalência, são geométricas todas as tesselações obtidas através do teorema 1.6.1.

Proposição 1.6.2 ([29, 30])**.** Qualquer tesselação τ de uma superfície $\mathbb{M}$ obtida pelo teorema 1.6.1 é equivalente a uma tesselação geométrica de $\mathbb{M}$.

Corolário 1.6.3. Seja $\mathbb{M}$ uma superfície orientável de gênus $g \geq 2$. Ademais, sejam $p_1, \cdots, p_t$, R, E, $V_1, \cdots, V_t$ inteiros positivos, tais que $R = \dfrac{4(g-1)\prod_j p_j}{(t-2)\prod_j p_j - \sum_i \prod_{j\neq i} p_j}$, $E = \dfrac{tR}{2}$ e $V_i = \dfrac{R}{2p_i}$. Nestas condições, existe uma tesselação semirregular $[2p_1, \cdots, 2p_t]$ de $\mathbb{M}$, com E arestas, R vértices, $F = \sum_i V_i$ faces, das quais $\dfrac{R}{2p_i}$ são $2p_i$-gons.

Em particular, quando $t = 3$, se p_1, p_2 e p_3, R, E, V_1, V_2, V_3 são inteiros positivos, tais que $R = \dfrac{4(g-1)p_1p_2p_3}{p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3}$, $E = \dfrac{3R}{2}$, $V_1 = \dfrac{R}{2p_1}$, $V_2 = \dfrac{R}{2p_2}$, $V_3 = \dfrac{R}{2p_3}$, existe uma tesselação semirregular $[2p_1, 2p_2, 2p_3]$ de $\mathbb{M}$, com E arestas, R vértices, $F = \dfrac{R}{2p_1} + \dfrac{R}{2p_2} + \dfrac{R}{2p_3}$ faces, das quais $\dfrac{R}{2p_1}$ são $2p_1$-gons, $\dfrac{R}{2p_2}$ são $2p_2$-gons e $\dfrac{R}{2p_3}$ são $2p_3$-gons. Esta configuração é particularmente útil para tratarmos dos códigos quânticos coloridos, no capítulo 5.

1.6.1 Propriedades Métricas de Tesselações Semirregulares de Superfícies Hiperbólicas

Proposição 1.6.4. Seja $\mathbb{M}$ uma superfície orientável de gênus $g \geq 2$, sobre a qual existe uma tesselação semirregular $[m_1, m_2, \cdots, m_t]$. Se l denota o comprimento de aresta, a_i o comprimento hiperbólico do apótema de cada m_i-gon, r_i o comprimento hiperbólico do raio da circunferência circunscrita a cada m_i-gon e, finalmente, se A_i denota a distância hiperbólica entre os incentros de um m_i-gon e um m_{i+1}-gon adjacentes, então:

$$\pi = \sum_{i=1}^{t} \operatorname{arcsen}\left(\frac{\cos\left(\frac{\pi}{m_i}\right)}{\cosh\left(\frac{l}{2}\right)}\right), \tag{1.15}$$

$$a_i = \operatorname{arcsenh}\left(\operatorname{tgh}\left(\frac{l}{2}\right)\operatorname{cotg}\left(\frac{\pi}{m_i}\right)\right), \tag{1.16}$$

$$r_i = \operatorname{arccosh}\left(\cosh\left(a_i\right)\cosh\left(\frac{l}{2}\right)\right), \tag{1.17}$$

$$A_i = a_i + a_{i+1}. \tag{1.18}$$

Demonstração: A relação1.15 foi obtida em [25, 19]. As demais decorrem da aplicação direta das relações 1.9, 1.2 e 1.1, respectivamente. □

Observação 1.6.5. Fixados os inteiros m_i, $i = 1, \cdots, t$, pode-se extrair uma solução em l, mesmo que numérica, da equação (1.15). Utilizaremos este recurso ao estudar os parâmetros, mais especificamente, as distâncias dos códigos de superfície subjacentes a estas tesselações.

Considerando uma construção similar à contida na figura 1.14, suponha que, para uma tesselação semirregular $[m_1, \cdots, m_t]$, $t = 2s+1$, tem-se o comprimento do apótema do m_i-gon igual a a_i e que A_i é a distância entre o incentro de um m_i-gon e um m_{i+1}-gon adjacentes.

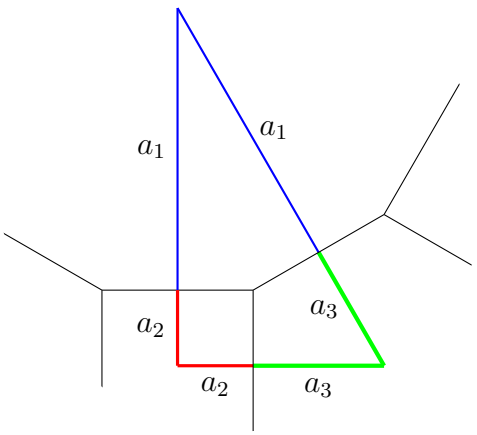


Figura 1.14: Vizinhança de um dos vértices de uma tesselação semirregular $[m_1, m_2, m_3]$

Independentemente da escolha de $j \in \{1, \cdots, t\}$, são válidas as seguintes igualdades:

$$\begin{aligned}
\sum_{k=0}^{2s}(-1)^k A_{j+k} &= \sum_{k=0}^{2s}\left((-1)^k a_{j+k} + (-1)^k a_{j+k+1}\right) \\
&= \sum_{k=0}^{2s}(-1)^k a_{j+k} + \sum_{k=0}^{2s}(-1)^k a_{j+k+1} \\
&= a_j + \left(\sum_{k=1}^{2s}(-1)^k a_{j+k}\right) + \left(\sum_{k=1}^{2s}(-1)^{k+1} a_{j+k}\right) + a_j \\
&= a_j + \left(\sum_{k=1}^{2s}(-1)^k a_{j+k}\right) - \left(\sum_{k=1}^{2s}(-1)^k a_{j+k}\right) + a_j \\
&= 2a_j.
\end{aligned}$$

ou seja, $A_j - A_{j+1} + A_{j+2} - \cdots - A_{j+2s-1} + A_{j+2s} = 2a_j$.

Disto decorre a proposição 1.6.6 abaixo. Apesar de não ter aplicação explícita no desenvolvimento do presente texto, esta se torna sensivelmente útil na implementação das rotinas computacionais que utilizamos nos bastidores do nosso estudo.

Proposição 1.6.6. Considere uma tesselação semirregular $\tau = [m_1, \cdots, m_t]$, $t = 2s+1$. Sejam A_i a distância entre o incentro de um m_i-gon e de um m_{i+1}-gon adjacentes e a_i o comprimento do apótema de cada m_i-gon. Então, para cada $j = 1, \cdots, t$, tem-se:

$$a_j = \sum_{k=0}^{2s}\frac{(-1)^k A_{j+k}}{2}$$

Em particular, quando $t = 3$, segue sendo $a_j = \dfrac{A_j - A_{j+1} + A_{j+2}}{2}$.

Observação 1.6.7. Em relação ao triângulo destacado na figura 1.15, o emprego direto da relação (1.2) fornece $l = 2\,\mathrm{arctgh}\left(\mathrm{senh}\,(a_i)\,\mathrm{tg}\left(\frac{\pi}{m_i}\right)\right)$, enquanto que o emprego da relação (1.4) fornece $r_i = \mathrm{arctgh}\left(\mathrm{tgh}\,(a_i)\,\mathrm{sec}\left(\frac{\pi}{m_i}\right)\right)$.

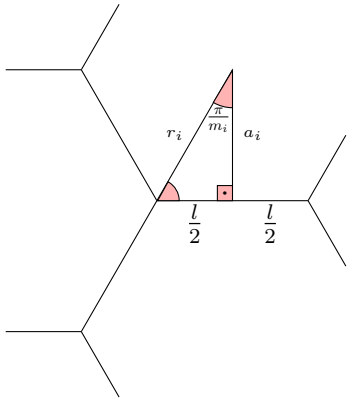


Figura 1.15: Vizinhança de um vértice da tesselação $[m_1, m_2, m_3]$, cujo comprimento de aresta é l. Destaca-se um triângulo hiperbólico de lados medindo $\frac{l}{2}$, a_i e r_i, respectivamente.

Proposição 1.6.8. A circunferência inscrita em um polígono hiperbólico regular tangencia cada uma das arestas deste exatamente no seu ponto médio.

A Proposição 1.6.8, cuja justificativa pode ser obtida na Observação 1.5.2, nos permite concluir que o segmento de geodésica que é determinado pelo incentro de dois polígonos adjacentes em uma tesselação semirregular, é ortogonal à aresta que estes polígonos têm em comum, conforme ilustra a Proposição 1.6.9 a seguir.

Proposição 1.6.9. Seja $[m_1, m_2, \cdots, m_t]$ uma tesselação semirregular do plano hiperbólico. O segmento de geodésica determinado pelos incentros de dois polígonos adjacentes é perpendicular à aresta que estes compartilham. Além do mais, seu comprimento hiperbólico coincide com a soma dos comprimentos hiperbólicos dos apótemas destes dois polígonos.

Proposição 1.6.10. Em uma tesselação hiperbólica semirregular $[m_1, m_2, m_3]$, se l é o comprimento de aresta, a_i é o comprimento hiperbólico do apótema de cada m_i-gon, r_i é o comprimento hiperbólico do raio da circunferência circunscrita a cada m_i-gon e se A_i é a distância hiperbólica entre os incentros de um m_i-gon e um m_{i+1}-gon adjacentes, então[7]:

[7] as operações com os índices são realizadas módulo 3

$$\begin{aligned} A_i &= \operatorname{arccosh}\left(\frac{\cos\left(\frac{2\pi}{m_i}\right)\cos\left(\frac{2\pi}{m_{i+1}}\right)+\cos\left(\frac{2\pi}{m_{i+2}}\right)}{\operatorname{sen}\left(\frac{2\pi}{m_i}\right)\operatorname{sen}\left(\frac{2\pi}{m_{i+1}}\right)}\right) \\ a_i &= \frac{A_i - A_{i+1} + A_{i+2}}{2} \\ r_i &= \operatorname{arctgh}\left(\operatorname{tgh}(a_i)\sec\left(\frac{\pi}{m_i}\right)\right) \\ l &= 2\operatorname{arctgh}\left(\operatorname{senh}(a_i)\ tg\left(\frac{\pi}{m_i}\right)\right) \end{aligned}$$

Demonstração: Com a segunda lei dos cossenos para triângulos hiperbólicos, garantimos que

$$A_i = \operatorname{arccosh}\left(\frac{\cos\left(\frac{2\pi}{m_i}\right)\cos\left(\frac{2\pi}{m_{i+1}}\right)+\cos\left(\frac{2\pi}{m_{i+2}}\right)}{\operatorname{sen}\left(\frac{2\pi}{m_i}\right)\operatorname{sen}\left(\frac{2\pi}{m_{i+1}}\right)}\right)$$

Agora, considere triângulo retângulo cuja hipotenusa mede r_i e os catetos medem $\frac{l}{2}$ e a_i respectivamente. Utilizando a relação (1.2), obtemos $l = 2\operatorname{arctgh}\left(\operatorname{senh}(a_i)\operatorname{tg}\left(\frac{\pi}{m_i}\right)\right)$. Utilizando a relação (1.4), obtemos $r_i = \operatorname{arctgh}\left(\operatorname{tgh}(a_i)\sec\left(\frac{\pi}{m_i}\right)\right)$. □

1.7 Fundamentos da Homologia

Considerando que a noção de homologia em superfícies seja muito mais abrangente do que precisamos para estabelecer o presente texto, estará sob o nosso foco apenas os conceitos homológicos necessários para o mesmo. Para uma leitura mais aprofundada acerca do tema, sugerimos [37], [32] ou [56]. A abordagem que utilizaremos é similar a de [8] e de [13].

Dada uma tesselação sobre uma superfície bidimensional $\mathbb{M}$, que estamos supondo ser compacta e orientável, designamos os vértices, arestas e faces subjacentes por 0-células, 1-células e 2-células, respectivamente. Seja $\mathfrak{C}_i$ o $\mathbb{Z}_2$-espaço vetorial livre, com base constituída por todas as i-células. A menos de um isomorfismo de espaços vetoriais, podemos considerar que uma cadeia $E = \sum a_j c_j$, onde $a_j \in \mathbb{Z}_2$ e c_j é uma i-célula, é obtida pela reunião de todas as i-células c_j para as quais $a_j \neq 0$. A operação de adição subjacente a este espaço vetorial é feita "coordenada a coordenada", isto é, $\sum a_j c_j + \sum a'_j c_j = \sum (a_j + a'_j) c_j$, o que coincide com a união disjunta de cadeias de i-células. A multiplicação por escalar é a óbvia. Dizemos que $\mathfrak{C}_i$ é o conjunto das i-cadeias. Para $i = 1, 2$, considere a aplicação $\mathbb{Z}_2$-linear $\partial_i : \mathfrak{C}_i \to \mathfrak{C}_{i-1}$ que

associa à cada i-célula a sua fronteira. Esta aplicação é comumente denominada na literatura por operador bordo. Quando não houver possibilidade de confusão, será omitido o subíndice.

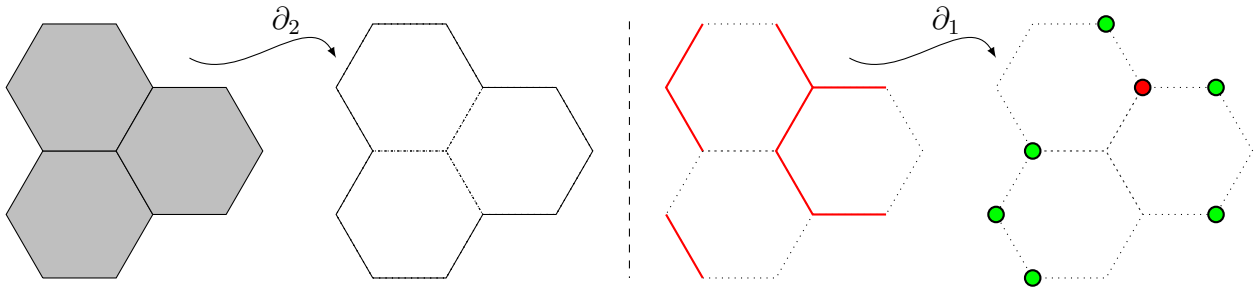


Figura 1.16: Ilustração da atuação dos operadores bordo: À esquerda, o operador ∂_2 associa à região sombreada, a sua fronteira. À direita, o operador ∂_1 associa ao conjunto de arestas, a sua fronteira. Nota-se que um vértice é "percebido"pelo operador ∂_1 se, e só se, este é pertencente a uma quantidade ímpar de arestas.

Uma propriedade relevante para a construção de códigos topológicos e a correção de erros diretamente ligada a estes pode ser ilustrada como segue: Se r é uma região composta pelas faces $f_1, \cdots, f_t$, a linearidade de ∂ nos garante que $\partial(r) = \sum \partial(f_j)$. Assim, um elemento da fronteira de f_j é um fator de $\partial(r)$ se, e só se, é uma aresta de uma única face componente da região r. Uma situação inteiramente análoga se passa com as arestas, vértices e a aplicação ∂_1. Em síntese, a aplicação ∂ associa a uma região as suas "divisas"e a uma reunião de arestas, os seus "pontos finais".

Tendo em vista que ∂_2 fornece as fronteiras de uma região, quando esta é simplesmente conexa, aquela é curva fechada. Sendo assim, não resta dúvidas de que $\partial \circ \partial = 0$. Isso garante que $Im(\partial_2) \subseteq Ker(\partial_1)$. Obviamente a igualdade nem sempre é válida. Vide figura 1.17.

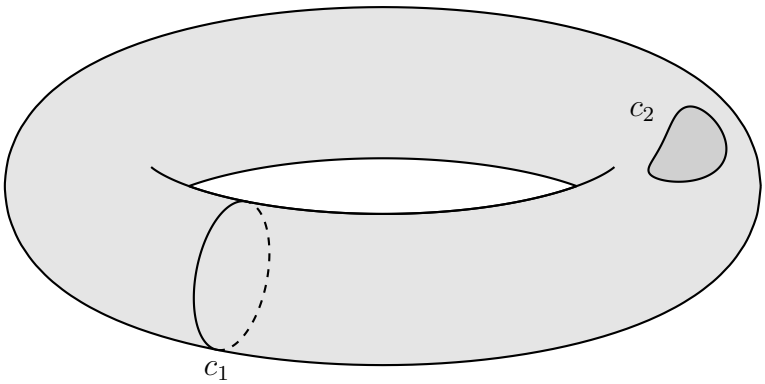


Figura 1.17: Duas curvas, c_1 e c_2, sobre o toro. Embora ambas as curvas estejam no núcleo do operador ∂_1, apenas c_2 está na imagem do operador ∂_2.

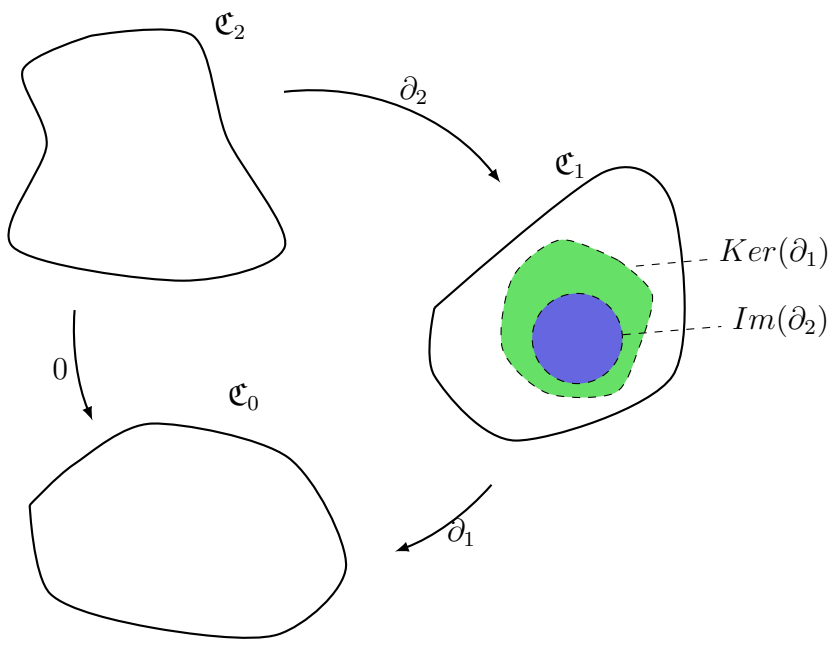


Figura 1.18: Diagrama ilustrando os operadores de bordo.

Definimos $\mathfrak{Z}_1 = Ker(\partial_1)$ e $\mathfrak{B}_1 = Im(\partial_2)$. Os elementos de $\mathfrak{Z}_1$ são denominados ciclos. Os ciclos são curvas fechadas, isto é, aquelas com fronteira nula. É visto que $\mathfrak{B}_1 \subseteq \mathfrak{Z}_1$.

O Primeiro Grupo de Homologia (de $\mathbb{M}$ sobre $\mathbb{Z}_2$) é o grupo $\mathfrak{H}_1 = \dfrac{\mathfrak{Z}_1}{\mathfrak{B}_1}$.

Proposição 1.7.1. Se $\mathbb{M}$ é uma superfície compacta e orientável, de gênus $g \geq 0$, então seu primeiro grupo de homologia, $\mathfrak{H}_1$, é isomorfo a $\mathbb{Z}_2^{2g}$.

A noção do primeiro grupo de homologia de uma superfície compacta e orientável identifica, via o quociente, os ciclos que diferem pela fronteira de uma região em $\mathfrak{C}_2$. Podemos estender esta noção para o quociente $\dfrac{\mathfrak{C}_1}{\mathfrak{B}_1}$, no qual duas curvas quaisquer, não necessariamente ciclos, pertencem a uma mesma classe de equivalência homológica se, e somente se, sua soma é fronteira de alguma região de $\mathfrak{C}_2$. Nosso interesse nesta construção residirá, em síntese, em codificar a informação em classes homológicas representadas por ciclos de homologia não trivial, de forma que erros constituídos por cadeias de homologia trivial não afetem a mesma.

Capítulo 2

Fundamentos da Mecânica Quântica

2.1 Axiomas da Mecânica Quântica

Nesta seção vamos discorrer sobre os quatro axiomas da mecânica quântica. Estes axiomas, que fundamentam toda a mecânica quântica, estabelecem os conceitos para a modelagem matemática de estados físicos de sistemas quânticos, a evolução destes sistemas através do tempo, os métodos de mensuração, e formas de acoplar dois ou mais sistemas quânticos a fim de estabelecer um sistema composto.

2.1.1 1º Axioma da Mecânica Quântica

Axioma 1. Dado um sistema físico isolado, existe um espaço de Hilbert, de forma que tal sistema é completamente determinado por vetores unitários deste espaço. O espaço de Hilbert é chamado de espaço dos estados do sistema, enquanto que os vetores unitários são chamados de vetores de estado.

Considerando que um espaço unidimensional consta de exatamente dois vetores unitários, estes não são adequados para descrever um sistema quântico. O sistema quântico mais simples é o do bit quântico, o qubit[1]. Este é um sistema físico que tem como espaço dos estados um espaço de Hilbert de dimensão dois e é o de maior interesse dentro computação quântica.

Considere agora um sistema físico a nível quântico, com espaço de estados $\mathcal{H}$, no qual é fixada uma base ortonormal $\{|0\rangle, |1\rangle\}$. Num sistema clássico simples, "0" e "1" são suficientes para descrever os dois únicos possíveis estados. Num sistema quântico, cada estado pode ter

[1] qubit é uma abreviação da língua inglesa para quantum bit

uma projeção não nula sobre cada um destes dois vetores, $|0\rangle$ e $|1\rangle$, haja visto que qualquer vetor unitário $|\varphi\rangle$ pode estar associado a algum estado do sistema. Este fenômeno é conhecido por superposição. Por exemplo, se $\{|\psi_i\rangle\}_i$ é uma base ortonormal de $\mathcal{H}$ e $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$, dizemos que o estado $|\psi\rangle$ é uma superposição quântica dos estados $|\psi_i\rangle$ e que α_i é a amplitude de $|\psi\rangle$ em relação ao estado $|\psi_i\rangle$. Vale ressaltar que uma condição necessária para que $|\psi\rangle$ seja uma superposição dos estados , é que $\sum_i |\alpha_i|^2 = 1$.

Denominamos por base computacional de $\mathcal{H}$ uma base ortonormal $\{|0\rangle, |1\rangle\}$ fixada.

Dado um estado $|\varphi\rangle$, existem $\gamma, \theta, \rho \in \mathbb{R}$, tais que $|\varphi\rangle = e^{i\gamma}\left(cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\rho}sen\left(\frac{\theta}{2}\right)|1\rangle\right)$. Conforme [44], o fator $e^{i\gamma}$ não fornece efeitos observáveis e, portanto, pode ser desconsiderado. Com isto, um estado $|\varphi\rangle$ pode ser completamente descrito, para finalidades físicas e computacionais, por $|\varphi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\rho}sen\left(\frac{\theta}{2}\right)|1\rangle$. Os parâmetros θ e ρ podem ser naturalmente associados a coordenadas esféricas, as quais, quando percorrem o intervalo $[0, \pi]$, determinam uma esfera unitária. A esta esfera comumente atribui-se a designação de Esfera de Bloch, a qual nos fornece um ponto de vista intuitivo do comportamento de um qubit.

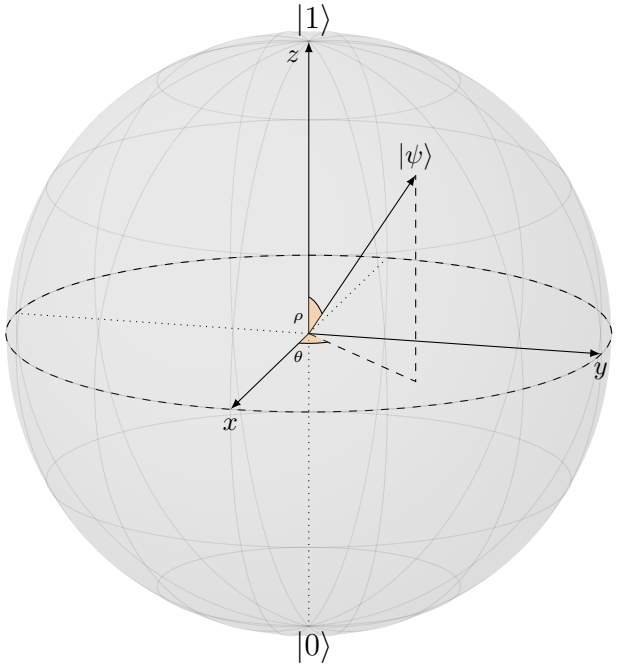


Figura 2.1: Esfera de Bloch e a representação do qubit $|\varphi\rangle = cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\rho}sen\left(\frac{\theta}{2}\right)|1\rangle$

Os estados $|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, $|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ também constituem uma base largamente

utilizada, a qual é conhecida como base conjugada. Nota-se que a atuação do operador $\mathfrak{H}$, descrito no exemplo 1.2.3-a, sobre a base computacional ocorre da seguinte maneira:

$$|0\rangle \overset{\mathfrak{H}}{\longmapsto} |+\rangle$$

$$|1\rangle \overset{\mathfrak{H}}{\longmapsto} |-\rangle$$

2.1.2 2º Axioma da Mecânica Quântica

Tão importante quanto a noção de estado de um sistema físico é o comportamento deste em relação ao tempo. Este tópico é contemplado pelo segundo axioma da mecânica quântica.

Axioma 2. Se $|\psi_0\rangle$ e $|\psi_1\rangle$ são vetores de estado de um determinado sistema quântico fechado, nos instantes de tempo t_0 e t_1, respectivamente, então existe um operador unitário $\mathcal{U}$, que atua sobre o espaço dos estados deste sistema, de forma que $|\psi_1\rangle = \mathcal{U}\,|\psi_0\rangle$. Tal operador $\mathcal{U}$ depende apenas de t_0 e de t_1.

Observação 2.1.1. O Axioma 2 pode ser reformulado como segue: A evolução através do tempo de um estado de um sistema quântico fechado é descrito pela Equação de Schrödinger:

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle$$

onde $\hbar$ é a constante de Planck e H é um operador Hermitiano fixado, conhecido como (operador) Hamiltoniano do sistema.

2.1.3 3º Axioma da Mecânica Quântica

Nos axiomas 1 e 2, estamos assumindo que o sistema físico em pauta está completamente isolado do ambiente que o contém, haja visto que tais sistemas são muito instáveis. Também assumimos que tais sistemas evoluem segundo algum operador unitário. Certamente a descrição e evolução de um sistema físico deve estar conectado a uma forma de extrair-se informações deste. Fechando tal lacuna, lançamos mão do terceiro axioma da mecânica quântica.

Axioma 3. Medições quânticas são descritas por uma coleção de Operadores de Medição, $\{M_m\}$. Cada operador M_m atua no espaço dos estados do sistema a ser medido. O índice m se refere ao possível resultado a ser obtido com a medição do sistema com o operador M_m. Se o estado do sistema é $|\varphi\rangle$ imediatamente antes da medição, são válidas as proposições:

i) A probabilidade de obter-se m com a medição é dada por $p(m) = \langle\varphi| M_m^\dagger M_m |\varphi\rangle$;

ii) O estado do sistema, imediatamente após a medição, é $\frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi| M_m^\dagger M_m |\varphi\rangle}}$;

iii) Os operadores de medição satisfazem a equação de completude: $\sum_m M_m^\dagger M_m = Id$;

iv) A equação de completude pode ser expressa, equivalentemente, por meio de soma de probabilidades, da seguinte maneira: $1 = \sum_m p(m) = \sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle\ ,\ \forall\, |\psi\rangle$.

Exemplo 2.1.2 ([44])**.** Considere um qubit pertencente a um espaço de estados $\mathcal{H}$, para o qual foi fixado uma base computacional. Considere os operadores $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. É fácil concluir que $M_0 + M_1 = Id$. Se estamos por mensurar o qubit $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, a probabilidade de obter-se com esta medição o valor 0 é descrita logo abaixo:

$$\begin{aligned}
p(0) &= \langle\varphi| M_0^\dagger M_0 |\varphi\rangle \\
&= \langle\varphi| M_0 |\varphi\rangle \\
&= \left(\sum_i \alpha_i |i\rangle\right)^\dagger M_0^\dagger M_0 \left(\sum_j \alpha_j |j\rangle\right) \\
&= \sum_{i,j} \alpha_i^* \alpha_j \langle i|\, 0\rangle \langle 0|\, j\rangle \\
&= \sum_{i,j} \alpha_i^* \alpha_j \delta_{i,0}\delta_{0,j} \\
&= \alpha_0^* \alpha_0 \\
&= |\alpha_0|^2
\end{aligned}$$

Analogamente, a probabilidade de obter-se o valor 1 com esta medição é $p(1) = |\alpha_1|^2$.

O estado verificado após a medição, em ambos os casos são, respectivamente:

$$\frac{M_0 |\varphi\rangle}{|\alpha_0|} = \frac{\alpha_0}{|\alpha_0|} |0\rangle \quad (2.1)$$

$$\frac{M_1 |\varphi\rangle}{|\alpha_1|} = \frac{\alpha_1}{|\alpha_1|} |1\rangle \quad (2.2)$$

Medições Projetivas: Levando em consideração que no âmbito da mecânica quântica, um observável é uma propriedade ou característica do sistema que pode ser mensurada através de operações físicas sobre tal, estamos em condições de definir as medições projetivas.

Uma medição projetiva é descrita por um observável M, que é um operador hermitiano que atua no espaço dos estados do sistema a ser observado. Dado que todo operador hermitiano é um operador normal, existe uma base ortonormal de tal espaço, constituída única e exclusivamente por autovetores de M. Se $M = \sum_m mP_m$ é a decomposição espectral de M, para cada autovalor m, o operador P_m é o projetor sobre o auto-espaço associado a m. Os valores possíveis de serem obtidos com essa medição são exatamente os autovalores de M.

Medindo-se um estado $|\varphi\rangle$, a probabilidade de obter-se m é $p(m) = \langle\varphi| P_m |\varphi\rangle$ e, caso o resultado da medição seja m, o estado do sistema imediatamente após a medição é $\frac{P_m |\varphi\rangle}{\sqrt{p(m)}}$.

Medições POVM: Do inglês positive operator-valued measure, as medições POVM são derivadas de uma medição usual, porém, com escrita ligeiramente mais elegante e prática.

Seja $\{M_m\}$ uma coleção de operadores de medição, conforme o axioma 3. A probabilidade de obter-se, através da referida medição, o valor m é $p(m) = \langle\varphi| M_m^\dagger M_m |\varphi\rangle$. Agora, se definirmos, para cada m, $E_m = M_m^\dagger M_m$, vemos que $\sum_m E_m = Id$, e que $p(m) = \langle\varphi| E_m |\varphi\rangle$.

2.1.4 4º Axioma da Mecânica Quântica

Os axiomas precedentes balizam a representação algébrica de um sistema quântico, sua evolução em relação ao tempo, bem como a maneira pela qual se pode observá-lo. Completando a base teórica, o quarto axioma descreve a maneira de acoplar dois ou mais sistemas.

Axioma 4. O espaço dos estados de um sistema físico composto é o produto tensorial dos

espaços de estados dos seus sistemas componentes. Além disto, num determinado instante, se um sistema físico é composto por n sistemas componentes e cada um destes sistemas se encontra no estado $|\varphi_i\rangle$, então o sistema composto se encontra no estado $|\varphi_1\rangle \otimes \cdots \otimes |\varphi_n\rangle$.

Embora o espaço dos estados de um sistema composto seja descrito algebricamente pelo produto tensorial dos espaços de estados subjacentes, um estado composto não é, necessariamente, obtido pelo produto tensorial de dois qubits. O melhor exemplo para ilustrar esta afirmação é encontrado nos chamados estados ou pares EPR (Einstein, Podolsky e Rosen), ou ainda, de estados de Bell. Estes estados são dados por $\beta_{|xy\rangle} = \frac{|0y\rangle + (-1)^x |1(y+1)\rangle}{\sqrt{2}}$:

$$\begin{aligned} \beta_{|00\rangle} &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad \beta_{|10\rangle} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ \beta_{|01\rangle} &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad \beta_{|11\rangle} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned}$$

Nenhum destes estados é obtido através do produto tensorial de dois estados de um qubit. A título de ilustração suponha, por absurdo, que existam estados $|u\rangle$ e $|v\rangle \in \mathcal{H}$, com a propriedade de que $\beta_{|00\rangle} = |u\rangle \otimes |v\rangle$, onde $|u\rangle = a_0 |0\rangle + a_1 |1\rangle$ e $|v\rangle = b_0 |0\rangle + b_1 |1\rangle$. Então,

$$\frac{|00\rangle + |11\rangle}{2} = a_0 b_0 |00\rangle + a_0 b_1 |01\rangle + a_1 b_0 |10\rangle + a_1 b_1 |11\rangle$$

de onde segue que $a_0 b_0 = a_1 b_1 = \sqrt{2}/2$ e $a_0 b_1 = a_1 b_0 = 0$.

Os estados $|\varphi\rangle$ de um espaço qualquer de mais de um qubit, é dito emaranhado quando não é possível decompor este estado em produtos tensoriais de estados de um único qubit.

Um fato sensivelmente interessante proveniente da utilização adequada de estados emaranhados é a chamada codificação superdensa. Realizar uma codificação superdensa, em poucas palavras, consiste em codificar uma quantidade q_0 de bits em q_1 qubits, onde $q_1 < q_0$.

Para ilustrar isso, suponha que duas estações, A e B, separadas fisicamente, estão de posse do estado $|\varphi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. Suponha, adicionalmente, que a estação A deseja enviar para a estação B, uma informação (clássica) em dois bits e que cada uma das estações está de posse de apenas um dos dois qubits de $|\varphi\rangle$. A codificação é feita sobre o operador $Id, \mathfrak{X}, i\mathfrak{Y}$ ou $\mathfrak{Z}$ que a estação A irá aplicar ao seu qubit, antes do envio para B, conforme a informação que deseja transmitir for $00, 01, 10$ ou 11, respectivamente. Ao receber este qubit já processado,

a estação B tem em mão um dos 4 estados EPR, os quais são ortogonais entre sí, e portanto, distinguíveis. Tendo em mãos a regra da codificação inicial utilizada pela estação A, a estação B consegue, então, reconhecer a informação de 2 bits enviada por A.

2.2 Operadores Densidade e Operações Quânticas

Um qubit é obtido pela superposição quântica de dois vetores de uma base ortonormal de $\mathcal{H} = \mathbb{C}^2$, enquanto que o estado de um sistema composto é obtido pelo produto tensorial dos estados de cada sistema componente, isto é, cada estado de um sistema físico quântico composto é um produto tensorial de qubits. Conhecendo cada estado de uma base ortonormal do sistema composto, é possível obter informações relativamente precisas sobre o estado do sistema. Como é de se imaginar, esta facilidade é apenas teórica, visto que na prática nem sempre se conhece tal base ou se tem um conjunto completo de informações sobre o sistema.

A princípio esta dificuldade deveria impossibilitar o trato da informação quântica, tendo em vista a eventual precisão que esta requer. Porém, para mitigar e/ou contornar esta situação adversa, lança-se mão dos Operadores Densidade, que nada mais são do que operadores $\rho = \sum_j p_j \left|\varphi_j\right\rangle \left\langle\varphi_j\right|$, onde $\{\left|\varphi_j\right\rangle\}_j$ é chamado de ensemble, enquanto que seus elementos são estados do sistema, tais que o estado do sistema $\left|\varphi\right\rangle$ se encontra no estado $\left|\varphi_j\right\rangle$ com probabilidade p_j. Este ensemble não necessariamente é uma base ou um subconjunto ortonormal de $\mathcal{H}$. Se $p_j \neq 0$ para um único j, dizemos que o qubit $\left|\varphi\right\rangle$ está num estado puro, caso contrário, dizemos que este qubit está num estado misto. Obviamente os adjetivos "puro"e "misto"atribuídos ao qubit estão relacionados ao ensemble utilizado.

Um estado de um sistema quântico difere daquele que este se encontrava num tempo passado apenas por um operador unitário, conforme garante o 2º Axioma da Mecânica Quântica. Com uma certa peculiaridade, podemos descrever a evolução de um sistema quântico que se encontra em um estado ρ, perante o tempo, tornando-se um estado ρ', da seguinte maneira:

$$\rho' = \Phi(\rho)$$

A aplicação Φ, que associa a um operador densidade ρ um novo operador densidade ρ',

chama-se de Operação Quântica. Uma operação quântica Φ é definida por $\Phi(\rho) = U\rho U^\dagger$, para algum operador U que atua sobre $\mathcal{H}$. Os casos que nos interessam são aqueles onde U é unitário, visto que representam a evolução do sistema em relação ao tempo, e a operação de medição, a qual é dada por um conjunto de observáveis $\{M_m\}$, de sorte que $\Phi(\rho) = M\rho M^\dagger$.

A fim de agregar conteúdo que seja útil a este texto às operações quânticas, consideremos o caso geral em que $\Phi(\rho) = \sum_j A_j \rho A_j^\dagger$. Esta é conhecida como Representação por Somatório da Operação Quântica Φ . Cada operador A_j é chamado de Elemento de Operação. Dada uma operação quântica Φ, cujos elementos de operação são A_j, é tal que $\sum_j A_j A_j^\dagger = Id$, dizemos que esta é uma operação quântica que preserva traço.

Os dois exemplos que seguem são extraídos da página 357 de [44].

Exemplo 2.2.1. Considere um estado puro $|\varphi\rangle$ que evolui segundo $|\varphi\rangle \mapsto U|\varphi\rangle$, onde U é um operador unitário. Seja $\rho = |\varphi\rangle\langle\varphi|$. Se $\varepsilon(\rho)$ é o operador densidade do sistema após tal evolução, tem-se $\varepsilon(\rho) = U\rho U^\dagger$.

Exemplo 2.2.2. Sabe-se que uma medição é implementada por um conjunto de operadores $\{M_m\}$, tais que $\sum_m M_m^\dagger M_m = Id$. Se o operador densidade do sistema imediatamente antes da mensuração é ρ e se definirmos $\varepsilon_m(\rho) = M_m \rho M_m^\dagger$, então segue que o operador densidade do sistema imediatamente após a mensuração é $\dfrac{\varepsilon_m(\rho)}{tr(\varepsilon_m(\rho))}$, enquanto que a probabilidade de obter-se m com tal medição é $p(m) = tr(\varepsilon_m(\rho))$.

2.3 Circuitos Quânticos e Portas Quânticas

Circuitos quânticos constituem uma ferramenta útil para a compreensão acerca da implementação de portas quânticas. Vamos discorrer brevemente sobre as principais portas quânticas, a fim de fixar notações e introduzir a linguagem. Para tal, sempre que possível ou útil, tentaremos estabelecer uma ligação com a computação clássica.

Um computador quântico tem um funcionamento essencialmente distinto do caso clássico. Neste, os transistores dão lugar às portas quânticas, que são operadores unitários e que atuam sobre o espaço dos estados do sistema. Estas portas são responsáveis por manipular

a informação quântica, a qual é proveniente de um estado físico, que nada mais é do que um conjunto de qubits, inicializados em estados conhecidos e previamente fixados. Ao passarem por cada porta quântica, estes estados (qubits) são eventualmente submetidos à aplicação do operador linear intrínseco à porta, transformando-os em novos estados (qubits). Este processo se repete tantas vezes quanto forem necessárias, de forma que ao "saírem"deste circuito e serem mensurados, tais qubits forneçam alguma informação que seja relevante.

Dado um operador U, o diagrama $|\varphi\rangle$ —[U]— representa a operação $|\varphi\rangle \mapsto U|\varphi\rangle$. A evolução do produto tensorial de dois ou mais vetores é representado mediante a adição de uma linha para cada componente. Vide figura 2.2.

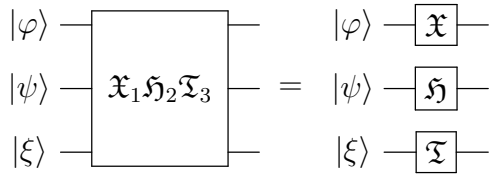


Figura 2.2: Dois circuitos quânticos equivalentes. Ambos representam a ação do operador $\mathfrak{X} \otimes \mathfrak{H} \otimes \mathfrak{T}$ sobre o estado composto determinado pelo vetor $|\varphi\rangle \otimes |\psi\rangle \otimes |\xi\rangle$.

Para um bit clássico $a \in \mathbb{Z}_2$, a operação NOT é aquela dada por $a \mapsto a + 1$. Fazendo papel análogo à operação NOT, temos a porta Bit Flip, determinada pelo operador de Pauli $\mathfrak{X}$: $\mathfrak{X}|a\rangle = |a \oplus 1\rangle$, $a \in \mathbb{Z}_2$. A porta quântica Phase Shift, ou Phase Flip, é aquela descrita pelo operador $\mathfrak{Z}$: $\mathfrak{Z}|a\rangle = (-1)^a|a\rangle, a \in \mathbb{Z}_2$. Este operador, tendo em vista que não se tem a noção de "sinal"em $\mathbb{Z}_2$, não tem análogo em bits clássicos.

Ao se tratar de sistemas clássicos de dois bits, existem, dentre outras, as operações lógicas AND ($AND(a,b) = ab$), OR ($OR(a,b) = ab \oplus a \oplus b$), XOR ($XOR(a,b) = a \oplus b$), NAND ($NAND(a,b) = 1 \oplus ab$) e NOR ($NOR(a,b) = (a \oplus 1)(b \oplus 1)$), descritas na tabela 2.1.

Note que nenhuma porta clássica é injetiva e, portanto, nem inversível. Já no caso quântico, tendo em vista que todo operador que estabelece uma porta quântica é unitário, segue, em particular, que são inversíveis.

Notemos, por um instante, que a porta XOR fornece o segundo bit, quando o primeiro é 0 e fornece o inverso do segundo bit, quando o primeiro é 1. Em síntese, $XOR(a,b) = NOT^a(b)$. Vale ressaltar que, para um operador linear $T : \mathbb{Z}_2 \to \mathbb{Z}_2$ qualquer, utilizamos a notação T^a denotando as possíveis potências de T, isto é, $T^0 = Id_{\mathbb{Z}_2}$ e $T^1 = T$.

Tabela 2.1: Portas lógicas que atuam em 2 bits

Bits	AND	OR	XOR	NAND	NOR
00	0	0	0	1	1
01	0	1	1	1	0
10	0	1	1	1	0
11	1	1	0	0	0

De forma análoga definimos o operador **CNOT**, cuja notação vem do inglês Controled-Not, e é dado por $\mathbf{CNOT}\,|a,b\rangle = |a\rangle \otimes \mathfrak{X}^a\,|b\rangle = |a, a \oplus b\rangle$, $a, b \in \mathbb{Z}_2$. Assim como no parágrafo cima, dado aqui um operador linear $T : \mathcal{H} \to \mathcal{H}$, utilizamos $T^0 = Id_{\mathcal{H}}$, enquanto que $T^1 = T$. A matriz da porta **CNOT**, bem como o símbolo que este emprega nos circuitos quânticos são fornecidos na Figura 2.3 logo abaixo.

$$\begin{array}{ll} |00\rangle & \overset{\mathbf{CNOT}}{\mapsto} |00\rangle \\ |01\rangle & \overset{\mathbf{CNOT}}{\mapsto} |01\rangle \\ |10\rangle & \overset{\mathbf{CNOT}}{\mapsto} |11\rangle \\ |11\rangle & \overset{\mathbf{CNOT}}{\mapsto} |10\rangle \end{array} \qquad \mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Figura 2.3: Da esquerda para a direita: Atuação da porta **CNOT** numa base computacional; Matriz do operador **CNOT**; Circuitos Quânticos Representando a Ação do Operador **CNOT**. No circuito, o qubit assinalado com um ponto preto é chamado de bit de controle, atuando como uma espécie de interruptor, e o qubit assinalado com o símbolo $\oplus$ é o qubit alvo, o qual é modificado, segundo a porta $\mathfrak{X}$, dependendo do qubit de controle.

A porta **CNOT** é, em essência, a porta $\mathfrak{X}$-controlada, no seguinte sentido: Dada uma porta U qualquer, chama-se de porta U-controlada à porta definida por $U_C\,|a,b\rangle = |a, U^a(b)\rangle$.

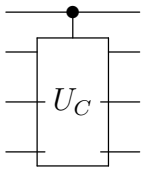


Figura 2.4: Representação da porta U-controlada.

A principal característica que difere a computação quântica da clássica é que esta primeira é, essencialmente, sequencial. É possível realizar computação paralela na computação clássica, porém, isto gera um custo computacional extra, necessitando-se de tantos processadores quanto a quantidade de linhas paralelas de processamento se deseja. Na computação

quântica, existe uma forma natural de se implementar a computação paralela, de maneira computacionalmente muito eficiente. Este feito é chamado de Paralelismo Quântico. O paralelismo quântico consiste em, dada uma função $f : \mathbb{Z}_2 \to \mathbb{Z}_2$, considerar a porta quântica U_f, que atua em dois qubits, $|x, y\rangle \overset{U_f}{\longmapsto} |x, y \oplus f(x)\rangle$. Inicializando o processamento em $\mathfrak{H}_1 |00\rangle = |00\rangle + |10\rangle$, o subproduto proveniente da porta U_f é $|0, f(0)\rangle + |1, f(1)\rangle$ [2]. Com isto, obtém-se informação sobre todos os valores possíveis que a função f assume. Fica clara a importância do paralelismo quântico quando a função f atua em mais do que 2 bits.

[2] Tecnicamente, $\dfrac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$

Capítulo 3

Códigos Quânticos Corretores de Erros

3.1 Códigos Quânticos Corretores de Erros

A informação quântica está armazenada em um estado físico de um sistema quântico. Este, por sua vez, é suscetível a interferências do ambiente que o cerca e pode facilmente ser levada ao colapso, fato que é conhecido como decaimento quântico ou decoerência quântica. A ferramenta utilizada para proteger a informação contra o decaimento quântico consiste nos códigos quânticos corretores de erros. Estes códigos compõem o escopo principal deste capítulo e são o cerne do presente trabalho.

Embora, como descrito acima, os códigos quânticos corretores de erros sejam empregados na proteção da informação quântica, seja no seu envio ou armazenamento, seu emprego também se dá no contorno e mitigação das imprecisões da dinâmica da computação, e.g., aqueles que são gerados por uma falha na codificação ou numa porta quântica. Por ora, estaremos assumindo que não existam erros na codificação da informação, bem como que o processamento desta por cada porta quântica empregada seja realizada de maneira perfeita, livre de erros. Como veremos mais adiante, é razoável supormos isso agora haja visto que os códigos quânticos corretores de erros protegem a informação contra tal interferência, também, desde que a probabilidade de ocorrer um erro, associada a cada porta, seja menor do que um determinado valor. Este feito é conhecido como Computação Tolerante à Falhas.

Um Código Quântico Corretor de Erros de comprimento n que codifica k qubits é, em síntese, um subespaço de dimensão 2^k de um espaço de Hilbert $\mathcal{C}$ cuja dimensão é 2^n. Assim como ocorre com os códigos clássicos corretores de erros, aqui também introduz-se uma

espécie de redundância, a qual viabiliza a detecção e posterior correção de erros, pelos quais a informação codificada tenha sido eventualmente acometida. Isso torna óbvio que $n > k$.

3.2 Erros, Síndrome de Erros e a Correção de Erros

Após codificada, a mensagem enviada ou armazenada, é submetida a uma medição quântica a fim de realizar uma detecção de erros. Os operadores empregados nesta medição são cuidadosamente escolhidos de forma que os resultados desta forneçam informações precisas sobre o tipo de erro que eventualmente tenha corrompido a mensagem codificada original. Os resultados desta medição quântica são conhecidos como síndromes de erro.

Tendo em vista que um computador quântico opera, em essência, a níveis de escala subatômica e que qualquer interferência pode facilmente corromper a informação, principalmente as provenientes do ambiente onde tal aparelho está alojado, podemos inferir que os erros são contínuos em relação ao tempo. De fato isto é observado por diversos autores e nos omitiremos em tratar a respeito deste assunto aqui .

Devido a esta continuidade do erro, uma das maiores benesses provenientes desta área e que torna factível a computação quântica, é a discretização do erro: É suficiente conhecer um conjunto finito de erros, com boas propriedades obviamente, e relativos aos quais estar munido de formas de identificar sua ocorrência, bem como conhecer a maneira apropriada para realizar a correção. Argumentaremos um pouco a fim de elucidar esta informação.

Suponha que um erro $\mathfrak{E}$ corrompa um qubit $|\varphi\rangle$, transformando-o em $\mathfrak{E}|\varphi\rangle$ e que o estado $|\varphi\rangle$ esteja associado ao operador densidade ρ. Sendo $\mathfrak{E}$ uma operação quântica que preserva traço, existem operadores E_m, tais que $\mathfrak{E}(\rho) = E_m \rho E_m^\dagger$. Para cada m, existem escalares $\alpha_{m,0}, \alpha_{m,1}, \alpha_{m,2}, \alpha_{m,3} \in \mathbb{C}$, tais que $E_m = \alpha_{m,0} Id + \alpha_{m,1}\mathfrak{X} + \alpha_{m,2}\mathfrak{Z} + \alpha_{m,3}\mathfrak{X}\mathfrak{Z}$, visto que $\{Id, \mathfrak{X}, \mathfrak{Z}, \mathfrak{X}\mathfrak{Z}\}$ é uma base de $M_2(\mathbb{C})$. Desta forma, o estado eventualmente não normalizado $\mathfrak{E}|\varphi\rangle$ pode ser escrito como superposição dos estados $|\varphi\rangle, \mathfrak{X}|\varphi\rangle, \mathfrak{Z}|\varphi\rangle, \mathfrak{X}\mathfrak{Z}|\varphi\rangle$.

Ao realizar uma medição quântica conveniente, este primeiro deve colapsar para algum dos quatro estados componentes da superposição. Identificando tal estado colapsado, basta eventualmente aplicar o operador de Pauli conveniente para recuperar o estado original $|\varphi\rangle$.

3.3 O Código Bit Flip

O código quântico corretor de erros mais elementar é o dito código bit flip e é baseado no código clássico de repetição. Similarmente ao código clássico supracitado, o código bit flip consiste em codificar um bit lógico $\varphi \in \{0,1\}$ em uma série de produtos tensoriais de $|\varphi\rangle$. Este código protege a informação contra a ação de erros do tipo bit flip ocorrendo em qualquer quantidade de qubits menor do que a metade da utilizada na codificação, visto que a decodificação é feita através do sistema de maior voto. A título de ilustração, considere a codificação $0 \mapsto |000\rangle$ e $1 \mapsto |111\rangle$. Suponha, adicional e provisoriamente, que ocorrem apenas erros do tipo bit flip ($\mathfrak{X}$), e no máximo em um dos três qubits. Se o estado $|\varphi\rangle$ é resultante da codificação, detecta-se um erro ocorrido em apenas um qubit simplesmente mensurando-se os projetores P_0, P_1, P_2 e P_3 listados abaixo:

$$\begin{aligned} P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111|, \\ P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011|, \\ P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101|, \\ P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|. \end{aligned}$$

Se tal medição fornece $j \in \{1,2,3\}$, fica evidente que o qubit φ_j do estado $|\varphi_1\varphi_2\varphi_3\rangle$ é distinto dos demais. Como estamos assumindo que eventualmente ocorrem erros em no máximo um qubit, pode-se concluir que este ocorreu no qubit φ_j. Agora, como estamos assumindo que ocorrem apenas erros bit flip, isto é, os decorrentes da ação do operador $\mathfrak{X}$, e considerando que $\mathfrak{X}^2 = Id$, basta aplicar $\mathfrak{X}_j$ ao estado atual a fim de corrigir o erro.

O circuito abaixo ilustra a codificação, detecção e posterior correção de erros do código bit flip com blocos de comprimento 3:

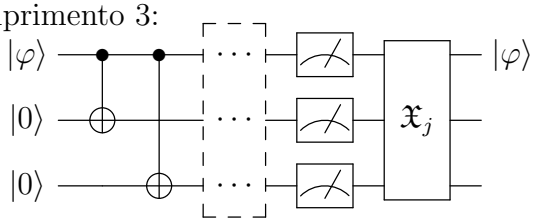


Figura 3.1: Circuito quântico ilustrando o código Bit Flip. O retângulo pontilhado indica o lapso temporal no qual a informação é, eventualmente, corrompida.

A medição citada acima identifica a síndrome de erro, a qual é explorada na seção 3.2. A síndrome identifica em qual, ou quais, qubits ocorreu o erro. Sabendo de antemão os

possíveis erros que podem ocorrer em cada qubit, basta aplicar ao estado quântico do sistema, imediatamente após a medição, operadores que eliminam o erro, obtendo assim, a informação original. A tabela abaixo ilustra a relação entre a síndrome e a correção de erros.

Saída da Medição	Erro	Correção
0	(Nenhum erro identificado)	(nenhuma ação a ser tomada)
1	Erro no 1^{o} qubit	Aplicar $\mathfrak{X}_1$
2	Erro no 2^{o} qubit	Aplicar $\mathfrak{X}_2$
3	Erro no 3^{o} qubit	Aplicar $\mathfrak{X}_3$

Embora o código bit flip explorado aqui seja completamente eficaz quando ocorre erro somente do tipo bit flip, e em no máximo um qubit, ele não corrige adequadamente erros em dois ou mais qubits, conduzindo, neste caso, a uma falha na informação.

Internamente a cada sistema físico que determina um qubit, suponha que a probabilidade de ocorrer um erro bit flip neste é p. Então, a probabilidade de que tal qubit não sofra erro é $1-p$. Dito isto e considerando o sistema de três qubits do código bit flip, a probabilidade de, por exemplo, somente os dois primeiros qubits sofrerem erro é de $p^2(1-p)$, haja visto que a probabilidade de o terceiro qubit permanecer intacto é $(1-p)$. Assim, a probabilidade de exatamente dois qubits sofrerem erro é de $3p^2(1-p)$. Esta probabilidade corresponde à soma das probabilidades de os dois primeiros, ou os dois últimos ou o primeiro e o último qubit sofrerem tal erro. A probabilidade de que os três qubits sofram erro é de p^3. Seja, então, p_e a probabilidade de 2 ou 3 qubits sofrerem erro do tipo bit flip. Tem-se:

$$p_e = 3p^2(1-p) + p^3 = 3p^2 - 2p^3.$$

3.4 O Código Phase Shift

Com certo exagero podemos dizer que os códigos Bit Flip e Phase Shift (ou Phase Flip) são, em essência, iguais. Obviamente que estes corrigem erros distintos - Bit Flip/ Phase shift- porém, o fazem de maneira muito similar.

O código Phase Shift consiste num código de repetição, que protege a informação de erros do tipo Phase Shift, que sabemos ser a ação do operador $\mathfrak{Z}$, do grupo de Pauli, em algum qubit. Como feito antes, e a título de exemplo, vamos considerar o código de 3 qubits, nos quais estamos supondo que pode ocorrer no máximo um erro, em um único qubit, e somente do tipo Phase Shift. A codificação para este código é dada por $0 \mapsto |+++\rangle\,,\ 1 \mapsto |---\rangle$. Abaixo temos um circuito que ilustra tal codificação.

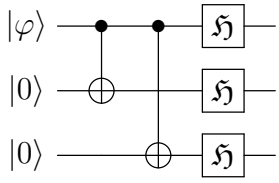


Figura 3.2: Circuito quântico ilustrando a codificação do código Phase Shift.

Os operadores utilizados na medição que fornece a síndrome de erros são os operadores $P'_j = \mathfrak{H}^{\otimes^3} P_j \mathfrak{H}^{\otimes^3}$, $j \in \{0,1,2,3\}$, e P_j são os operadores utilizados nas medições relacionadas aos códigos bit flip. O protocolo de correção de erros, baseado na síndrome, é:

Resultado da Medição	Erro	Correção
0	(Nenhum erro identificado)	(nenhuma ação a ser tomada)
1	Erro no $1^{\underline{o}}$ qubit	Aplicar $\mathfrak{Z}_1$
2	Erro no $2^{\underline{o}}$ qubit	Aplicar $\mathfrak{Z}_2$
3	Erro no $3^{\underline{o}}$ qubit	Aplicar $\mathfrak{Z}_3$

3.5 O Código de Shor

O código de Shor, aqui abordado, foi publicado por Peter W. Shor em 1995, em [48]. Temos um ótimo resumo deste código em [50] e em [44] .

O Código de Shor é um código de nove qubits que protege a informação contra erros bit flip e phase shift, desde que este ocorra em, no máximo, um único qubit. A construção deste código consiste, basicamente, da concatenação dos códigos bit flip e phase shift.

A codificação do Código de Shor é iniciada com a mesma codificação implementada no código Phase Shift: $|0\rangle \mapsto |+++\rangle\,,\ |1\rangle \mapsto |---\rangle$. Em seguida, cada um destes três qubits

é novamente codificado, agora com o circuito da codificação do código bit flip. Visto que, mediante este processo, tem-se $|+\rangle \mapsto \dfrac{|000\rangle + |111\rangle}{\sqrt{2}}$, e $|-\rangle \mapsto \dfrac{|000\rangle - |111\rangle}{\sqrt{2}}$, segue que a codificação do código de Shor é realizada da seguinte forma:

$$\begin{aligned} |0\rangle &\mapsto = \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}} \\ |1\rangle &\mapsto = \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}} \end{aligned}$$

Abaixo está o circuito de codificação do código de Shor.

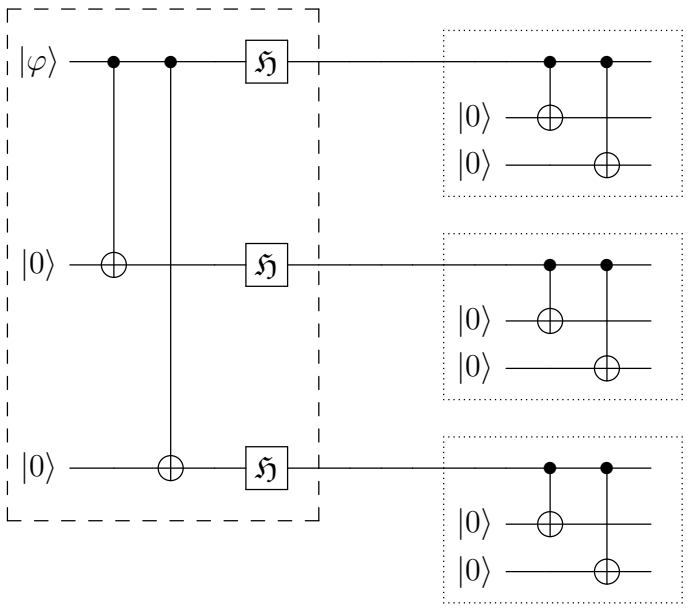


Figura 3.3: Circuito quântico ilustrando a codificação do código de Shor: No retângulo maior, tracejado, encontra-se a codificação Phase Shift, enquanto que nos três retângulos menores, pontilhados, encontram-se codificações Bit Flip.

Considerando que o estado pode ser visto como três blocos de três qubits cada, os operadores responsáveis pela medição e apuração da síndrome de erros bit flip são $\mathfrak{Z}_j\mathfrak{Z}_{j+1}$ e $\mathfrak{Z}_{j+1}\mathfrak{Z}_{j+2}$, $j \in \{1,2,3\}$ - estes comparam os qubits dentro de cada bloco. Caso algum erro seja detectado, a recuperação é feita mediante a aplicação do operador $\mathfrak{X}$ no qubit corrompido. Os operadores responsáveis pela medição e apuração de síndrome de erros do tipo phase shift são os operadores $\mathfrak{X}_1\mathfrak{X}_2\mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_6$ e $\mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_8\mathfrak{X}_9$. Estes observáveis comparam os sinais entre o primeiro e o segundo e entre o segundo o terceiro blocos, respectivamente. Caso algum erro seja detectado neste processo, basta aplicar o operador $\mathfrak{Z}$ em qualquer um dos

três qubits do bloco corrompido.

3.6 Os Códigos CSS

Um código CSS - o nome é uma homenagem aos seus desenvolvedores: Calderbank-Shor-Steane - é baseado em artefatos da computação clássica, com a devida adaptação ao nosso escopo, o da computação quântica. Mais especificamente, um código CSS é baseado em códigos lineares clássicos. Exploramos na seção abaixo os fundamentos necessários para o desenvolvimento e a compreensão deste tema.

O Código CSS

Sejam $\mathcal{C}_1$ e $\mathcal{C}_2$ códigos clássicos lineares sobre $\mathbb{Z}_2$, cujos parâmetros são $[n, k_1]$ e $[n, k_2]$, respectivamente, tais que $k_1 > k_2$, $\mathcal{C}_2 \subset \mathcal{C}_1$ e que $\mathcal{C}_1$ e $\mathcal{C}_2^{\perp}$ corrigem, no mínimo, t erros cada. O código CSS de $\mathcal{C}_1$ sobre $\mathcal{C}_2$, que é denotado por $CSS(\mathcal{C}_1, \mathcal{C}_2)$, é um código quântico de parâmetros $[n, k_1 - k_2]$, que é capaz de corrigir erros em até t qubits, conforme visto a seguir.

Dada uma palavra $x \in \mathcal{C}_1$, define-se o estado quântico $|x + \mathcal{C}_2\rangle$ da seguinte maneira:

$$|x + \mathcal{C}_2\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x + y\rangle$$

Note que se $x, x' \in \mathcal{C}_1$, de forma que $x - x' \in \mathcal{C}_2$, tem-se $|x + \mathcal{C}_2\rangle = |x' + \mathcal{C}_2\rangle$. Para cada $x \in \mathcal{C}_1$, o estado $|x + \mathcal{C}_2\rangle$ depende somente da classe lateral representada por x em $\mathcal{C}_1/\mathcal{C}_2$. Sejam, ainda, $x, x' \in \mathcal{C}_1$, tais que $|x + \mathcal{C}_2\rangle = |x' + \mathcal{C}_2\rangle$. É fácil ver que $x - x' \in \mathcal{C}_2$. Isto implica que sempre que x, x' pertencem a classes laterais distintas de $\mathcal{C}_1/\mathcal{C}_2$, os estados $|x + \mathcal{C}_2\rangle$ e $|x' + \mathcal{C}_2\rangle$ são ortogonais.

O código quântico $CSS(\mathcal{C}_1, \mathcal{C}_2)$ é definido como sendo o subespaço de $\mathcal{H}$, que é um espaço de Hilbert de dimensão 2^n, gerado pelos vetores $\{|x + \mathcal{C}_2\rangle\}_{x \in \mathcal{C}_1}$. O número de coclasses de $\mathcal{C}_1/\mathcal{C}_2$ é $\dfrac{|\mathcal{C}_1|}{|\mathcal{C}_2|} = 2^{k_1 - k_2}$, a qual é a dimensão de $CSS(\mathcal{C}_1, \mathcal{C}_2)$.

Um código quântico CSS detecta e corrige até t erros, utilizando-se das propriedades de correção e detecção de erros dos códigos (clássicos) $\mathcal{C}_1$ e $\mathcal{C}_2$.

Exemplo 3.6.1 (Código de Steane)**.** O código de Steane pode ser visto como um código CSS. Para tal, seja $\mathcal{C}$ o código linear clássico que tem a matriz de Hamming H, explicitado no exemplo 1.1.3. Basta, então, definir $\mathcal{C}_1 = \mathcal{C}$ e $\mathcal{C}_2 = \mathcal{C}^{\perp}$.

3.7 Códigos Estabilizadores

Ao longo desta seção estudaremos brevemente os códigos estabilizadores, os quais foram idealizados por Daniel Gottesman, [34, 35].

Como antes, $\mathcal{H}$ denota um espaço de Hilbert de dimensão n, sobre o qual age $\mathcal{P}_n$, o grupo de Pauli de n qubits.

Observação 3.7.1. Quaisquer dois operadores de $\mathcal{P}_n$ ou comutam, ou anticomutam.

Diremos que um conjunto de geradores de um grupo $\mathcal{S}$ é um conjunto de geradores independente quando o grupo gerado pelos remanescentes, após removido qualquer um de seus elementos, é um subgrupo próprio do primeiro, isto é, se $\mathcal{S} = \langle g_1, \cdots, g_{i-1}, g_i, g_{i+1}, \cdots, g_l \rangle \supsetneq \langle g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_l \rangle$, para algum $i = 1, \cdots, l$.

Seja $\mathcal{S}_{est}$ um subgrupo abeliano de $\mathcal{P}_n$, tal que $-Id \notin \mathcal{S}_{est}$ e seja $\mathcal{V}_{\mathcal{S}_{est}}$ o subespaço de $\mathcal{H}$ que é estabilizado por $\mathcal{S}_{est}$.

Proposição 3.7.2. Seja $\mathcal{S}_{est} = \langle g_1, \cdots, g_l \rangle$, um grupo gerado por l geradores independentes, de modo que $-Id \notin \mathcal{S}_{est}$. Para cada $i = 1, \cdots, l$, existe $g \in \mathcal{P}_n$, tal que $g g_i g^{\dagger} = -g_i$ e $g g_j g_j^{\dagger} = g_j$, para cada $j \neq i$.

Demonstração: Ver proposição 10.4 de [44]. □

Proposição 3.7.3. Seja $\mathcal{S}_{est}$ um subgrupo abeliano de $\mathcal{P}_n$, tal que $-Id \notin \mathcal{S}_{est}$ e que $g_1, \cdots, g_{n-k}$ constituem um conjunto de geradores independentes deste. Nestas condições, o subespaço de $\mathcal{H}$ estabilizado por $\mathcal{S}_{est}$ tem dimensão igual a 2^k.

Demonstração: Ver proposição 10.5 de [44]. □

Corolário 3.7.4. Seja $\mathcal{S}_{est}$ um subgrupo abeliano do grupo de Pauli $\mathcal{P}_n$, de ordem 2^r, tal que $-Id \notin \mathcal{S}_{est}$. Seja d o peso mínimo dentre os pesos dos operadores de $N(\mathcal{S}_{est}) - \mathcal{S}_{est}$. Então o

espaço dos estados $\mathcal{V}_{\mathcal{S}_{est}}$, que é estabilizado por $\mathcal{S}_{est}$ é um código quântico corretor de erros, cujos parâmetros são $[n, k, d]$, onde $k = n - r$.

Seja $|\varphi\rangle$ um estado estabilizado por $\mathcal{S}_{est}$, isto é, $|\varphi\rangle \in \mathcal{V}_{\mathcal{S}_{est}}$. Se um eventual erro ε corrompe este estado, esta ação pode ser detectada mensurando-se com os geradores de $\mathcal{S}_{est}$, obtendo-se assim, uma síndrome de erros: Se o erro ε anticomuta com um dos geradores, este leva $|\varphi\rangle$ em um subespaço ortogonal ao espaço estabilizado, visto que $|\varphi\rangle$ é um autovetor associado ao autovalor 1 de cada um dos g_j. Caso contrário, o espaço é estabilizado. Desta maneira, é possível identificar e, posteriormente, corrigir o erro.

Devemos nos ater ao fato de que se um erro ε, que corrompe a informação, pertence ao centralizador do grupo estabilizador, não é detectado pelo código estabilizador.

No teorema seguinte temos uma condição para que um conjunto de erros seja corrigível. Neste, vamos considerar um subgrupo abeliano $\mathcal{S}_{est} \subset \mathcal{P}_n$, que estabiliza o espaço $\mathcal{V}$ de um espaço de Hilbert $\mathcal{H}$, com a condição de que $-Id \notin \mathcal{S}_{est}$.

Teorema 3.7.5 (Condições para Correção de Erros para Códigos Estabilizadores)**.** *Seja $\mathcal{S}_{est}$ o grupo estabilizador do código estabilizador $\mathcal{V}_{\mathcal{S}_{est}}$. Adicionalmente, seja $\{E_j\}$ um conjunto de operadores de $\mathcal{P}_n$, tal que $E_j^\dagger E_k \notin \mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$, para cada j, k. Então, $\{E_j\}$ é um conjunto de erros corrigíveis de $\mathcal{V}_{\mathcal{S}_{est}}$.*

Demonstração: Ver teorema 10.8 de [44].□

Exemplo 3.7.6 (O Código Bit Flip)**.** Considere $\mathcal{S}_{est} = \langle \mathfrak{Z}_1\mathfrak{Z}_2, \mathfrak{Z}_1\mathfrak{Z}_3, \mathfrak{Z}_2\mathfrak{Z}_3 \rangle$. Ocorrido um erro $\mathfrak{X}_j$ no estado $|\varphi\rangle \in \mathcal{V}_{\mathcal{S}_{est}}$, o estado $\mathfrak{X}_j |\varphi\rangle$ é ortogonal ao espaço estabilizado pelos operadores $\mathfrak{Z}_j\mathfrak{Z}_{j+1}$ e $\mathfrak{Z}_{j-1}\mathfrak{Z}_j$, onde as operações com os índices são feitas módulo 3. Com isto, obtem-se uma síndrome de erros e, consequentemente, realiza-se a correção: Aplica-se ao estado corrompido, o operador $\mathfrak{X}_j$.

Exemplo 3.7.7. (O Código de Steane) O Código de Steane, tratado no exemplo 3.6.1 é, em particular, um código estabilizador. O Grupo estabilizador do código de Steane é o grupo $\mathcal{S}_{est} = \langle g_1, \cdots, g_6 \rangle$, onde cada g_j é dado na tabela abaixo:

$$
\begin{aligned}
g_1 &= \mathfrak{X}_4 X \mathfrak{X}_5 \mathfrak{X}_6 \mathfrak{X}_7, & g_4 &= \mathfrak{Z}_4 \mathfrak{Z}_5 \mathfrak{Z}_6 \mathfrak{Z}_7, \\
g_2 &= \mathfrak{X}_2 \mathfrak{X}_3 \mathfrak{X}_6 \mathfrak{X}_7, & g_5 &= \mathfrak{Z}_2 \mathfrak{Z}_3 \mathfrak{Z}_6 \mathfrak{Z}_7, \\
g_3 &= \mathfrak{X}_1 \mathfrak{X}_3 \mathfrak{X}_5 \mathfrak{X}_7, & g_6 &= \mathfrak{Z}_1 \mathfrak{Z}_3 \mathfrak{Z}_5 \mathfrak{Z}_7.
\end{aligned}
$$

Suponha que o estado inicial $|\varphi\rangle$ seja corrompido[1] por um erro ε. Realizando uma medição que nos fornece a informação sobre este erro, no sentido de que o estado corrompido está, ou não, no espaço estabilizado por cada um dos geradores de $\mathcal{S}_{est}$, isoladamente, obtemos uma síndrome de erros, o qual nos permite identificar e, posteriormente, corrigir o erro.

A título de exemplo, suponha que o estado corrompido $\varepsilon\,|\varphi\rangle$ não seja estabilizado pelo operador g_1. Isto nos diz que ocorreu um erro phase shift em um dos últimos 4 qubits. Se, contudo, $\varepsilon\,|\varphi\rangle$ não é estabilizado por g_2, sabemos, então, que o erro phase shift ocorreu num dos dois último qubits, haja visto que estamos considerando que, no máximo, um qubit é afetado por este. Se, finalmente, $\varepsilon\,|\varphi\rangle$ não é estabilizado por g_3, o erro phase shift ocorreu no último qubit; se $\varepsilon\,|\varphi\rangle$ seja estabilizado por g_3, o erro phase shift ocorreu no sexto qubit. As demais ocasiões são analisadas de maneira similar.

Como as medições realizadas com os observáveis g_j não afetam o estado quântico, basta aplicar o operador de correção adequado, recuperando assim a informação original.

3.7.1 Operadores Lógicos e Distância de um Código Estabilizador

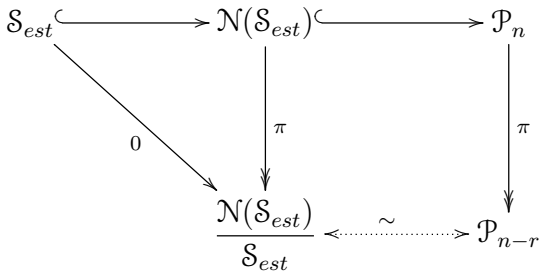
É sabido que o código Bit Flip é um código estabilizador, cujo grupo estabilizador é o grupo $\mathcal{S}_{est} = \langle \mathfrak{Z}_1\mathfrak{Z}_2, \mathfrak{Z}_2\mathfrak{Z}_3 \rangle$, haja visto que $\mathfrak{Z}_1\mathfrak{Z}_2 \cdot \mathfrak{Z}_2\mathfrak{Z}_3 = \mathfrak{Z}_1\mathfrak{Z}_3$. Assim, este código codifica um qubit lógico, segundo $|x\rangle_L \mapsto |xxx\rangle$, $x \in \mathbb{Z}_2$. Estes estados são denominados de estados lógicos. Note que $\mathfrak{Z}_1\,|0\rangle_L = |0\rangle_L$, mas que $\mathfrak{Z}_1\,|1\rangle_L = -\,|1\rangle_L$. Por este motivo dizemos que $\mathfrak{Z}_1$ é um operador $\mathfrak{Z}$ codificado ou o Operador lógico $\mathfrak{Z}$, o qual é denotado por $\bar{\mathfrak{Z}}$. Considere agora o operador $\mathfrak{Z}_2$, que é obtido pelo produto dos operadores $\mathfrak{Z}_1\mathfrak{Z}_2 \in \mathcal{G}$ por $\mathfrak{Z}_1$. Observe que $\mathfrak{Z}_2\,|0\rangle_l = |0\rangle_L$ e que $\mathfrak{Z}_2\,|1\rangle_L = -\,|1\rangle_L$. Assim, a atuação dos operadores $\mathfrak{Z}_1$ e $\mathfrak{Z}_2$ sobre este código é idêntica. Estes representam, portanto, o mesmo operador lógico. Obviamente existe um operador lógico do tipo $\bar{\mathfrak{X}}$, a saber, $\mathfrak{X}_1\mathfrak{X}_2\mathfrak{X}_3$, ou qualquer outro obtido do produto deste

[1] Consideremos aqui caso geral, onde ε pode ser o operador identidade

com um operador qualquer de $\mathcal{S}_{est}$. Da mesma forma, o operador $\mathfrak{Y}_1\mathfrak{X}_2\mathfrak{X}_3$ é um operador $\mathfrak{Y}$ codificado. Em síntese, qualquer elemento do quociente $\frac{\mathcal{N}(\mathcal{S}_{est})}{\mathcal{S}_{est}}$ é um operador lógico. É possível mostrar que $\frac{\mathcal{N}(\mathcal{S}_{est})}{\mathcal{S}_{est}}$ é um grupo isomorfo ao grupo de Pauli de 1 qubit.

Tome um operador lógico g. Existem operadores $s \in \mathcal{S}_{est}$ e $h \in \mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$, de modo que $g = sh$. Assim, g preserva o espaço do código, porém não atua trivialmente sobre ele. Note que, dentre estes operadores de $\mathcal{N}(\mathcal{S}_{est})$, o peso mínimo que se encontra é 1, e é dado, por exemplo, pelo operador $\mathfrak{Z}_1$. Este valor é a distância do código Bit Flip.

De modo geral, seja $\mathcal{S}_{est} = \langle g_1, \cdots, g_r \rangle$, $g_j \in \mathcal{P}$, um grupo abeliano para o qual $\{g_1, \cdots, g_r\}$ é um conjunto de geradores independentes, e que satisfaz a restrição de que $-Id \notin \mathcal{S}_{est}$. Seja $\mathcal{V}_{\mathcal{S}_{est}}$ o código estabilizador associado a $\mathcal{S}_{est}$. Cada classe de $\frac{\mathcal{N}(\mathcal{S}_{est})}{\mathcal{S}_{est}}$ é um operador lógico codificado, representada por qualquer um de seus elementos. É possível provar que este grupo quociente é isomorfo ao grupo de Pauli de $k = n - r$ qubits, $\mathcal{P}_k$, isto é, tal grupo é gerado por $\bar{\mathfrak{X}}_1, \bar{\mathfrak{Z}}_1, \cdots, \bar{\mathfrak{X}}_k, \bar{\mathfrak{Z}}_k$.



Pode-se decompor $\mathcal{P}_n$ em três classes disjuntas $\mathcal{P}_n = (\mathcal{P}_n - \mathcal{N}(\mathcal{S}_{est})) \cup (\mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}) \cup \mathcal{S}_{est}$. Os operadores de $\mathcal{S}_{est}$ não oferecem risco algum ao estado que contém a informação, visto que este pertence ao espaço estabilizado, em particular, por aquele operador. Um operador de $\mathcal{P}_n - \mathcal{N}(\mathcal{S}_{est})$ anti-comuta com pelo menos um operador de $\mathcal{S}_{est}$, portanto, está relacionado a algum erro que pode ser identificado e corrigido. Agora, um operador de $\mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$ causa um erro que não é detectado. Conforme [10], a distância de um código quântico é o menor valor d para o qual o código não detecta d erros. Desta forma, a distância de um código estabilizador consiste no peso do operador de $\mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$ que possui menor peso. Em síntese, a distância de um código estabilizador é o menor peso obtido comparando-se os pesos de todos os representantes de cada um dos operadores lógicos.

Observação 3.7.8. Denotamos por $[n, k, d]$ os parâmetros de um código quântico corretor

de erros $\mathcal{C}$, que codifica k qubits lógicos em n qubits físicos e cuja distância é d.

Embora esta forma de estabelecer a distância de um código estabilizador pareça pouco construtiva, o que para o trabalho que estamos desenvolvendo poderia ter pouca utilidade, podemos estabelecer uma maneira prática de construir os operadores lógicos de qualquer código estabilizador de uma maneira que a implementação computacional seja factível.

Para tal feito considere, para cada $x = (x_i)_i, z = (z_i)_i \in \mathbb{Z}_2^n$, o vetor (x, z) definido por $(x_1, \cdots, x_n, z_1, \cdots, z_n) \in \mathbb{Z}_2^{2n}$ e, para cada $v = (x, z) \in \mathbb{Z}_2^{2n}$, o operador $\sigma_v = \sigma_{(x,z)} = \bigotimes_{j=1}^n i^{x_j z_j} \mathfrak{X}^{x_j} \mathfrak{Z}^{z_j}$. Segue que $\sigma_u \sigma_v = \Phi(u^t \Omega v) \sigma_v \sigma_u$, onde $\Omega = \begin{pmatrix} 0 & Id \\ -Id & 0 \end{pmatrix}$ é a matriz $2n \times 2n$ dada em blocos e $\Phi(\theta) = e^{i\pi\theta}$, [10]. Conhecendo $x_{g_j}, z_{g_j} \in \mathbb{Z}_2^n$, tais que $\sigma_{(x_{g_j}, z_{g_j})} = g_j$, para cada $j = 1, \cdots, r$, é fácil reconhecer e listar todos os operadores lógicos, bem como cada um de seus representantes. Observando os pesos destes operadores, facilmente se reconhece o peso do código estabilizador, estabilizado por $\mathcal{S}_{est}$.

3.8 Códigos Topológicos

Os códigos estabilizadores englobam diversos códigos anteriormente conhecidos e, adicionalmente, fornecem uma maneira sucinta de descrição e compreensão destes. Iniciaremos agora o estudo de uma subclasse destes códigos, que são conhecidos como códigos topológicos.

Estamos interessados em explorar maneiras de codificar e armazenar informações com uma determinada liberdade topológica. Os códigos topológicos tem uma representatividade quanto ao trato da informação quântica haja visto que cada elemento do grupo estabilizador atua não trivialmente em uma pequena quantidade de qubits e, similarmente, cada qubit está no suporte de uma pequena quantidade de elementos do grupo estabilizador. Esta característica é especialmente importante quando deseja-se implementar uma computação tolerante à falhas, visto que uma porta quântica defeituosa eventualmente corrompe apenas uma pequena quantidade de qubits.

Os códigos topológicos são, em particular, códigos estabilizadores. Assim, fazem-se necessárias algumas construções geométricas e combinatórias, estabelecidas com o intuito de

construir famílias de códigos estabilizadores.

3.8.1 O Código Tórico

Dado $l > 0$, qualquer reticulado do 1-toro composto por $l \times l$ quadrados, conforme ilustrado na figura 3.5, pode ser associado a um código quântico corretor de erros, de maneira canônica. Este processo, que vamos descrever aqui, foi idealizado por Alexei Yurievich Kitaev, [40]. Cada código desta família é conhecido como Código Tórico.

Considere o toro gerado pelo quociente do plano euclidiano pelo quadrado cujo lado mede 1 unidade, o qual é uma região fundamental para o grupo de translações inteiras do plano.

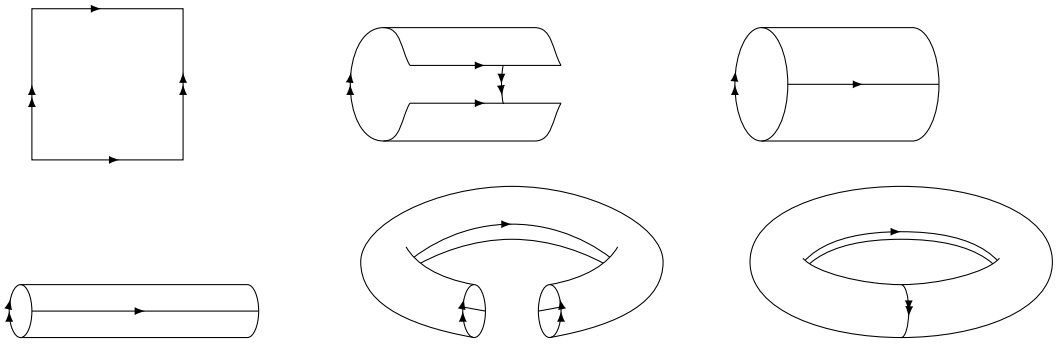


Figura 3.4: Processo de identificação dos lados opostos de um retângulo que fornece o 1-toro

O reticulado quadrado $l \times l$ sobre o 1-toro possui l^2 faces, $2l^2$ arestas e l^2 vértices.

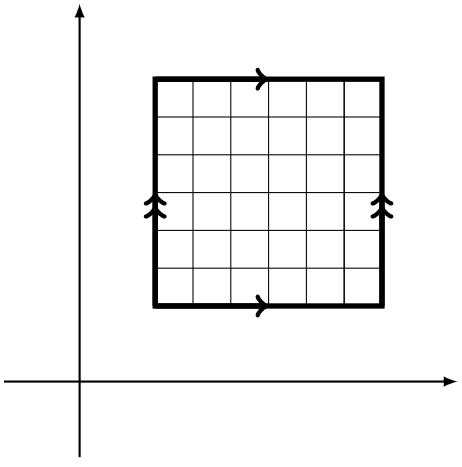


Figura 3.5: Reticulado 6×6 sobre o 1-toro.

Indexando cada uma das arestas, digamos, $e_1, \cdots, e_{2k^2}$, e considerando o espaço de Hil-

bert $\mathcal{V} = \bigotimes_{j=1}^{2k^2} \mathbb{C}^2$, podemos associar a cada aresta e_j, um qubit do j-ésimo fator de $\mathcal{V}$. Desta forma, podemos construir os geradores do grupo estabilizador do código em pauta, os quais são comumente denominados na literatura por operadores vértice e operadores face, respectivamente, como segue: Dados um vértice $v \in \mathcal{V}$ e uma face $f \in \mathcal{F}$, define-se

$$\mathfrak{Z}_v = \bigotimes_{e \in \mathcal{E}} \mathfrak{Z}^{\delta(v \in \partial(e))} \quad \mathfrak{X}_f = \bigotimes_{e \in \mathcal{E}} \mathfrak{X}^{\delta(e \in \partial(f))}$$

A figura 3.6 ilustra um operador face, associado à face f, e um operador vértice, associado ao vértice v, ambos estabelecidos sobre o toro.

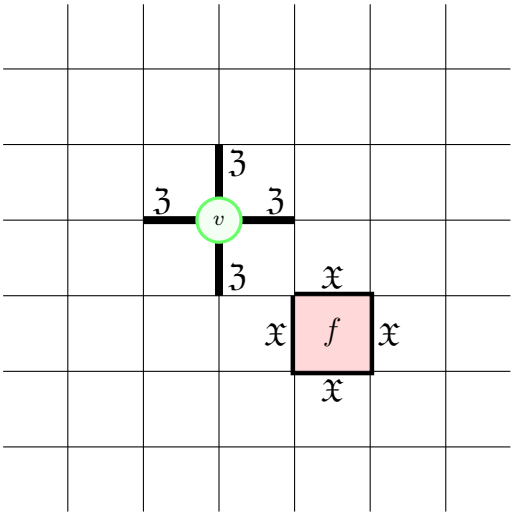


Figura 3.6: Suportes dos operadores associados à face f e ao vértice v, respectivamente.

O grupo estabilizador do código tórico é o grupo $\mathcal{S}_{est} = \langle \mathfrak{X}_f, \mathfrak{Z}_v;\ v \in \mathcal{V},\ f \in \mathcal{F} \rangle$. É fácil ver que $\mathcal{S}_{est}$ é um grupo abeliano, pois o suporte de um operador face intersecta o suporte de um operador vértice ou em zero ou em duas arestas. Obviamente, $-Id \notin \mathcal{S}_{est}$.

Observando-se a construção destes operadores, é fácil notar que $\prod_{f \in \mathcal{F}} \mathfrak{X}_f = \prod_{v \in \mathcal{V}} \mathfrak{Z}_v = Id_{\mathcal{S}_{est}}$. Desta forma, $\mathcal{S}_{est}$ possui $2l^2 - 2$ geradores independentes. Assim, o espaço estabilizado por $\mathcal{S}_{est}$ é um código quântico estabilizador, cuja dimensão é 2^k, onde $k = n - r$, $n = \#\mathcal{E} = 2l^2$ e $r = 2l^2 - 2$, ou seja, $k = 2$. Portanto, o código tórico codifica 2 qubits em $n = 2l^2$ qubits.

A fim de determinar a distância do código tórico, precisamos conhecer os operadores lógicos subjacentes, isto é, aqueles operadores que comutam com a totalidade de elementos

do grupo estabilizador, mas que não pertencem a este. Para tal, dada qualquer 1-cadeia c, com $c = \sum e \in \mathcal{E}\delta_{(e\in c)}e$, considere os operadores $\mathfrak{X}_c = \bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in c)}$ e $\mathfrak{Z}_c = \bigotimes_{e\in\mathcal{E}} \mathfrak{Z}^{\delta(e\in c)}$. Qualquer operador do grupo de Pauli de n qubits, $\mathcal{P}_n$, que atua sobre $\mathcal{H}$ é, portanto, determinado pelo produto $\mathfrak{X}_c\mathfrak{Z}_c$, para alguma 1-cadeia c, a menos uma constante de fase i^α, onde $\alpha \in \mathbb{Z}_4$.

Suponha que uma 1-cadeia c prefixada é tal que $v \in \partial(c)$. Desta forma, a cardinalidade do conjunto $\mathcal{E}_v \cap \mathcal{E}_c$ é ímpar. Dito isto, consideramos o desenvolvimento que segue:

$$\begin{aligned}
\mathfrak{Z}_c\mathfrak{X}_f &= \left(\bigotimes_{e\in\mathcal{E}} \mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\right)\left(\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\
&= \bigotimes_{e\in\mathcal{E}} \left(\mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\
&= \bigotimes_{e\in\mathcal{E}} \left((-1)^{\delta(e\in\mathcal{E}_f)\delta(e\in\mathcal{E}_c)}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\right)\\
&= \prod_{e\in\mathcal{E}}(-1)^{\delta(e\in\mathcal{E}_f)\delta(e\in\mathcal{E}_c)} \bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\\
&= \left(\prod_{e\in\mathcal{E}} \left((-1)^{\delta(e\in\mathcal{E}_f\cap\mathcal{E}_c)}\right)\right) \bigotimes_{e\in\mathcal{E}} \left(\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\right)\\
&= \left(\prod_{e\in\mathcal{E}}(-1)^{\delta(e\in\mathcal{E}_f\cap\mathcal{E}_c)}\right)\mathfrak{X}_f\mathfrak{Z}_c\\
&= \left(\prod_{e\in\mathcal{E}}(-1)^{\delta(e\in\mathcal{E}_f\cap\mathcal{E}_c)}\right)\left(\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\left(\bigotimes_{e\in\mathcal{E}} \mathfrak{Z}^{\delta(e\in\mathcal{E}_c)}\right)\mathfrak{X}_f\mathfrak{Z}_c\\
&= (-1)^{\sum_{e\in\mathcal{E}} \delta(e\in\mathcal{E}_f\cap\mathcal{E}_c)}\mathfrak{X}_f\mathfrak{Z}_c
\end{aligned}$$

Assim, $\mathfrak{Z}_c\mathfrak{X}_f = \mathfrak{X}_f\mathfrak{Z}_c$ se, e somente se, $\sum_{e\in\mathcal{E}} \delta(e \in \mathcal{E}_f \cap \mathcal{E}_c) \equiv 0(mod 2)$. Notando que $\sum_{e\in\mathcal{E}} \delta(e \in \mathcal{E}_f \cap \mathcal{E}_c) = \#\mathcal{E}_f \cap \mathcal{E}_c$, segue que se $\delta(c) \neq 0$, então $\mathfrak{Z}_c\mathfrak{X}_f \neq \mathfrak{X}_f\mathfrak{Z}_c$, para cada $f \in \mathcal{F}$, tal que $\mathcal{E}_f \cap \partial(c) \neq \emptyset$ e, com isto, $\mathfrak{Z}_c \notin \mathcal{N}(\mathcal{S}_{est})$.

A tesselação dual do reticulado $l \times l$ do toro pode ser obtida rotacionando-se cada aresta deste, num sentido predeterminado, em 90 graus e sobre o seu ponto médio, fazendo assim, cada face dar lugar a um vértice e vice-versa. Assim, podemos associar qualquer operador $\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{A}\subset\mathcal{E})}$ a uma 1-cadeia c pertencente à tesselação direta e, similarmente, associar qual-

quer operador $\bigotimes_{e\in\mathcal{E}} \mathfrak{Z}^{\delta(e\in\mathcal{A}\subset\mathcal{E})}$ a uma 1-cadeia c^* na tesselação dual. Qualquer operador de Pauli em n qubits $g \in \mathcal{P}_n$ pode, portanto, ser escrito como $g = i^\alpha \mathfrak{X}_c \mathfrak{Z}_c^*$, $\alpha \in \mathbb{Z}_4$.

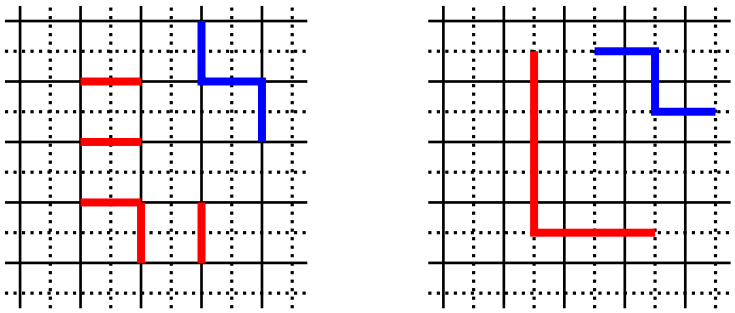


Figura 3.7: Duas representações de dois operadores do tipo $\mathfrak{Z}_c$: à esquerda, a representação canônica, enquanto que à direita, a representação na tesselação dual. Cada aresta da 1-cadeia c, associada ao suporte do operador $\mathfrak{Z}_c$, intersecta uma aresta de c^*, da 1-cadeia da sua representação dual. Estas intersecções ocorrem exatamente sobre as arestas que estão relacionadas aos qubits do suporte deste operador.

Note que, se $b \in \mathfrak{C}_1$ e $c^* \in \mathfrak{C}_1^*$, os operadores $\mathfrak{X}_b$ e $\mathfrak{Z}_{c^*}$ comutam se, e só se, as curvas determinadas por b e c^* se intersectam no máximo em um número par de pontos. Em particular, dada uma face $f \in \mathcal{F}$ e $c^* \in \mathfrak{C}_1^*$, ocorre que $\mathfrak{X}_f \mathfrak{Z}_{c^*} = -\mathfrak{Z}_{c^*} \mathfrak{X}_f$ se, e só se, $\partial^*(c^*) \bigcap Int(f) \neq \emptyset$, isto é, se um ponto da fronteira de c^* está situado sobre a face f. Este argumento é suficiente para garantir que, dada qualquer curva $c^* \in \mathfrak{C}_1^*$, o operador $\mathfrak{Z}_{c^*}$ pertence ao normalizador (centralizador) do grupo $\mathcal{S}_{est}$ se, e só se, $\partial^*(c^*) = 0$. Analogamente, para qualquer $c \in \mathfrak{C}_1$, $\mathfrak{X}_c \in \mathcal{N}$ se, e só se, $\partial(c) = 0$.

Os ciclos, sejam no reticulado direto, ou no dual, podem ser classificados em duas classes, quanto à homologia: Ciclos de homologia trivial e ciclos de homologia não trivial. Os ciclos de homologia trivial são curvas fechadas, que delimitam uma reunião de faces e este é obtido pela soma formal das arestas das faces que este delimita. Agora, um ciclo que possui homologia não trivial não pode ser obtido desta maneira. Em síntese, se c é um ciclo de homologia não trivial, $\mathfrak{X}_c \in \mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$. Fenômeno análogo ocorre no reticulado dual.

Portanto, cada ciclo de homologia não trivial, seja no reticulado direto ou dual, fornece um representante de um operador lógico. Tomando o menor peso destes operadores, obtemos o peso do código tórico associado a esta tesselação (ou reticulado). Note que o menor ciclo de homologia não trivial tem comprimento l. Desta forma, fica claro que o código tórico associado ao reticulado $l \times l$ sobre o toro é um código $[2l^2, 2, l]$.

3.8.2 Códigos de Superfície

Uma generalização dos códigos tóricos para superfícies orientáveis é concebida na forma de códigos simpléticos, utilizando mergulhos de grafos em tal superfície, em [10]. Conforme [40, 21], é possível generalizar a construção de códigos quânticos topológicos, estabelecendo tais construções sobre superfícies orientáveis compactas, cujo gênero é $g \geq 2$.

Baseado em [16, 15, 20], vemos em [21] uma importante construção acerca de códigos topológicos estabelecidos sobre superfícies, os quais estamos denominando por códigos de superfície. Em tal trabalho encontra-se a construção de códigos quânticos topológicos concebidos a partir de uma tesselação de uma superfície hiperbólica, cuja característica de Euler é negativa: Sobre uma superfície de gênero $g \geq 2$, a qual é homeomorfa ao g-toro e é obtida pelo quociente do plano hiperbólico pelo grupo de aplicações conformes, subjacente à tesselação regular $\{4g, 4g\}$ estabelecida sobre tal plano. Tendo em vista que o operador de projeção deste quociente é, localmente, uma isometria, a métrica estabelecida sobre tal superfície é hiperbólica. Por tanto, as tesselações consideradas em tal trabalho são hiperbólicas.

Consideremos a tesselação regular $\{p, q\}$ sobre $\mathbb{M}$, o g-toro de gênero $g \geq 2$. As equações 1.10 e 1.11 fornecem a quantidade de faces, vértices e arestas que compõem esta tesselação. Tais valores são ingredientes para a obtenção dos parâmetros dos códigos que ora estamos considerando. Para fixar notação, sejam $\mathcal{F}$, $\mathcal{E}$ e $\mathcal{V}$ os conjuntos de faces, arestas e vértices, respectivamente, de uma tesselação regular $\{p, q\}$ prefixada. Para cada $v \in \mathcal{V}$, considere $\mathcal{E}_v = \{e \in \mathcal{E} / v \in \partial(e)\}$ e, similarmente, para cada $f \in \mathcal{F}$, considere $\mathcal{E}_f = \{e \in \mathcal{E} / e \in \partial(f)\}$.

Com o intuito de estabelecer um código quântico topológico de superfície, para cada $f \in \mathcal{F}$, defina o operador $\mathfrak{X}_f = \bigotimes_{e \in \mathcal{E}} \mathfrak{X}^{\delta(e \in \mathcal{E}_f)}$ e, similarmente, para cada $v \in \mathcal{V}$, defina o operador $\mathfrak{Z}_v = \bigotimes_{e \in \mathcal{E}} \mathfrak{Z}^{\delta(e \in \mathcal{E}_v)}$. Estes operadores atuam sobre $\mathcal{H} = \mathbb{C}^{2n}$, onde $n = \#\mathcal{E}$. Observa-se que, para cada $v \in \mathcal{V}$ e para cada $f \in \mathcal{F}$, os conjuntos $\mathcal{E}_f$ e $\mathcal{E}_v$ possuem zero ou dois elementos em comum e, portanto, $\mathfrak{X}_f$ e $\mathfrak{Z}_v$ comutam. Desta forma o grupo gerado por $\mathfrak{X}_f, f \in \mathcal{F}$ e $\mathfrak{Z}_v, v \in \mathcal{V}$, $\mathcal{S}_{est} = \langle \mathfrak{X}_f, \mathfrak{Z}_v \rangle$, é um grupo abeliano.

Denote por $\mathcal{C}$ o subespaço vetorial de $\mathcal{H}$, obtido pela intersecção dos auto-espaços associados ao autovetor $+1$, de cada um destes operadores:

$$\mathcal{C} = \{|\varphi\rangle \in \mathcal{H} / \mathfrak{X}_f |\varphi\rangle = \mathfrak{Z}_v |\varphi\rangle = |\varphi\rangle, f \in \mathcal{F}, v \in \mathcal{V}\}$$

Tem-se, nestas condições, que $\mathcal{C}$ é o espaço estabilizado por $\mathcal{S}_{est}$.

Conforme observado pelos idealizadores deste código, $\prod_{f\in\mathcal{F}} \mathfrak{X}_f = \prod_{v\in\mathcal{V}} \mathfrak{Z}_v = Id$. Com isto, para cada $f_0 \in \mathcal{F}$, tem-se:

$$\begin{aligned}
\prod_{f\in\mathcal{F}, f\neq f_0} \mathfrak{X}_f &= \prod_{f\in\mathcal{F}, f\neq f_0} \left(\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)} \right) \\
&= \bigotimes_{e\in\mathcal{E}} \left(\prod_{f\in\mathcal{F}, f\neq f_0} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)} \right) \\
&= \bigotimes_{e\in\mathcal{E}} \left(\mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})} \prod_{f\in\mathcal{V}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)} \right) \\
&= \left(\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})} \right) \left(\bigotimes_{e\in\mathcal{E}} \prod_{f\in\mathcal{F}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)} \right) \\
&= \left(\bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})} \right) \left(\prod_{f\in\mathcal{V}} \bigotimes_{e\in\mathcal{E}} \mathfrak{X}^{\delta(e\in\mathcal{E}_f)} \right) \\
&= \mathfrak{X}_{f_0} \prod_{f\in\mathcal{F}} \mathfrak{X}_f \\
&= \mathfrak{X}_{f_0} Id \\
&= \mathfrak{X}_{f_0}
\end{aligned}$$

Analogamente, para cada $v_0 \in \mathcal{V}$ fixada, tem-se $\prod_{v\in\mathcal{V}, v\neq v_0} \mathfrak{Z}_v = \mathfrak{Z}_{v_0}$.

Assim, $\mathcal{S}_{est}$ possui $\#\mathcal{F}-1+\#\mathcal{V}-1$ geradores independentes. Portanto, o código $\mathcal{C}$ codifica $k = n - (\#\mathcal{F} + \#\mathcal{V} - 2)$ qubits. Logo,

$$\begin{aligned}
k &= n - (\#\mathcal{F} + \#\mathcal{V} - 2) \\
&= \#\mathcal{E} - \#\mathcal{F} - \#\mathcal{V} + 2 \\
&= -(\#\mathcal{F} - \#\mathcal{E} + \#\mathcal{V}) + 2 \\
&= -\chi(\mathbb{M}) + 2 \\
&= -2(1-g) + 2 \\
&= 2g
\end{aligned}$$

Em detrimento do código tórico, neste código de superfície, assim como nos próximos a serem explorados, não conseguimos estabelecer exatamente a distância, mas sim um limi-

tante inferior para esta. Este limitante é obtido estimando-se a um limitante inferior para a distância de grafo de um ciclo de homologia não trivial, dentre os situados tanto na tesselação direta quanto na tesselação dual. Na prática, é obtido tomando-se o menor inteiro, não menor do que o quociente da distância hiperbólica entre dois lados opostos do polígono da tesselação $\{4g, 4g\}$ pelo comprimento de aresta da tesselação. Obviamente compara-se com o mesmo quociente em relação à tesselação dual e utiliza-se o menor dentre estes dois valores como ingrediente para a determinação de tal limitante inferior para a distância do código. Note que, nesta construção, os princípios já estabelecidos no código tórico acerca de um operador pertencer, ou não, a $\mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$ são análogos.

Conforme 1.5.12, a distância hiperbólica entre um par de arestas opostas de um polígono da tesselação $\{4g, 4g\}$ é $d_{\mathbb{M}} = 2\,\text{arccosh}\left[\text{cotg}\left(\frac{\pi}{4g}\right)\right]$, enquanto que o comprimento de aresta de uma tesselação regular $\{p, q\}$ é $l = 2\,\text{arccosh}\left[\cos\left(\frac{\pi}{p}\right)\text{cossec}\left(\frac{\pi}{q}\right)\right]$, visto na equação 1.12, e o comprimento de aresta na tesselação dual, $\{q, p\}$ é igual a $2a$, onde a é o comprimento hiperbólico do apótema de um polígono da tesselação direta e é dado, conforme equação 1.13, por $a = \text{arccosh}\left[\text{cossec}\left(\frac{\pi}{p}\right)\cos\left(\frac{\pi}{q}\right)\right]$, ambas relações obtidas na proposição 1.5.10.

Assim, se d é a distância do código, segue que $d \geq \lceil min\{\frac{d_{\mathbb{M}}}{l}, \frac{d_{\mathbb{M}}}{2a}\}\rceil$.

Para ilustrar este processo, tomemos a tesselação regular $\{7, 3\}$ situada sobre o 2-toro. O comprimento de aresta desta tesselação é $l = 2\,\text{arccosh}\left[\cos\left(\frac{\pi}{7}\right)\text{cossec}\left(\frac{\pi}{3}\right)\right]$, enquanto que o diâmetro de um dos p-gons que determinam as faces é $2a = 2\,\text{arccosh}\left[\cos\left(\frac{\pi}{3}\right)\text{cossec}\left(\frac{\pi}{7}\right)\right]$. Assim, sabendo que o comprimento hiperbólico de um menor ciclo de homologia não trivial sobre o 2-toro é $d_{\mathbb{M}} = 2\,\text{arccos}\,h\left[\text{cotg}\left(\frac{\pi}{8}\right)\right]$, o código de superfície construído a partir desta, tem distância $d \geq \left\lceil min\left\{\frac{2\,\text{arccos}\,h\left[\text{cotg}\left(\frac{\pi}{8}\right)\right]}{2\,\text{arccosh}\left[\cos\left(\frac{\pi}{7}\right)\text{cossec}\left(\frac{\pi}{3}\right)\right]}, \frac{2\,\text{arccos}\,h\left[\text{cotg}\left(\frac{\pi}{8}\right)\right]}{2arccosh\left[\cos\left(\frac{\pi}{3}\right)\text{cossec}\left(\frac{\pi}{7}\right)\right]}\right\}\right\rceil$. Numericamente tem-se $d \geq 2,8033$, de onde seque que $d \geq 3$ pois, é um inteiro maior do que $2,8033$. Note que esta tesselação é composta por 42 arestas, assim, tem-se $n = 42$ qubits codificando $k = 4$ qubits, garantindo desta forma que este é um código $[42, 4, 3]$.

3.8.3 Códigos Coloridos

Os códigos coloridos foram introduzidos em [9], os quais partiam de tesselações euclidianas. Mais tarde, esta noção foi estabelecida sobre superfícies hiperbólicas, como visto em [50, 51].

Faremos uma breve introdução aos códigos quânticos coloridos abaixo, de forma que este trecho sirva de pré-requisito para a nossa construção posterior. Toda esta seção é baseada, principalmente, nas referências citadas neste parágrafo.

De modo geral, um código colorido é um código estabilizador construído a partir de uma tesselação sobre uma superfície, a qual deve ter valência 3 e ser 3-colorível. Uma tesselação ter valência 3 é sinônimo de que cada vértice componente desta possui valência 3, enquanto que ser 3-colorível é, por sua vez, sinônimo de que para cada face pode-se associar um símbolo do conjunto $\{R, G, B\}$, de forma que quaisquer duas faces adjacentes sejam associadas a símbolos distintos. Os símbolos escolhidos fazem referência às cores vermelho, verde e azul, respectivamente. Esta escolha provê o adjetivo "colorível" à tesselação.

Eventualmente o exemplo mais simples de tesselação 3-valente e 3-colorível é a tesselação regular $\{6, 3\}$ sobre o 1-toro, exibida na figura 3.8.

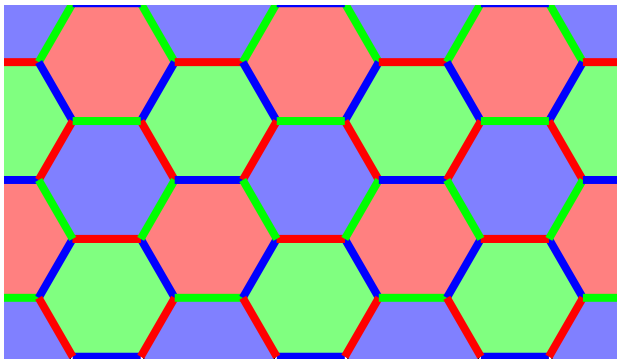


Figura 3.8: Tesselação regular $\{6, 3\}$, 3-valente e 3-colorível, do o 1-toro . Nota-se que de cada face emanam arestas associadas à mesma cor sua, enquanto que nenhuma face possui arestas cuja cor é mesma sua.

Diferentemente dos códigos de superfície, o código colorido é construído situando-se um qubit em cada um de seus vértices, e ao invés de os geradores do grupo estabilizador estarem determinados por vértices e faces, agora estão determinados em quantidade de dois por cada face, mediante a construção explanada logo a diante. Para fixar notações, considere, para cada $v \in \mathcal{V}$, o operador $\mathfrak{X}_{(v)}$ que é aquele cujo suporte é constituído apenas pelo qubit relacionado ao vértice v. Analogamente define-se o operador $\mathfrak{Z}_{(v)}$. Os geradores do grupo estabilizador $\mathcal{S}_{est}$ do código colorido são os operadores face, $\mathfrak{X}_{(f)}$ e $\mathfrak{Z}_{(f)}$, construídos da seguinte maneira:[2]

[2]Utilizam-se os parêntesis na notação $\bullet_{(*)}$ para distinguir da similar utilizada nos códigos de superfície.

$$\mathfrak{X}_{(f)} = \prod_{v \in f} \mathfrak{X}_{(v)}, \quad \mathfrak{Z}_{(f)} = \prod_{v \in f} \mathfrak{Z}_{(v)}.$$

Denotando por $\mathcal{F}_R$, $\mathcal{F}_G$ e $\mathcal{F}_B$ os subconjuntos de $\mathcal{F}$ compostos pelas faces vermelhas, verdes e azuis, respectivamente, podemos escrever as seguintes relações:

$$\prod_{f \in \mathcal{F}_R} \mathfrak{X}_{(f)} = \prod_{f \in \mathcal{F}_B} \mathfrak{X}_{(f)} = \prod_{f \in \mathcal{F}_G} \mathfrak{X}_{(f)}, \quad \prod_{f \in \mathcal{F}_R} \mathfrak{Z}_{(f)} = \prod_{f \in \mathcal{F}_B} \mathfrak{Z}_{(f)} = \prod_{f \in \mathcal{F}_G} \mathfrak{Z}_{(f)}.$$

Desta forma, escolhidas faces $f_r \in \mathcal{F}_R$ e $f_b \in \mathcal{F}_B$, escrevemos $\mathfrak{X}_{(f_r)} = \prod_{f \in \mathcal{F}_R / \{f_r\}} \mathfrak{X}_{(f)} \prod_{f \in \mathcal{F}_G} \mathfrak{X}_{(f)}$ e, similarmente, $\mathfrak{X}_{(f_b)} = \prod_{f \in \mathcal{F}_B / \{f_b\}} \mathfrak{X}_{(f)} \prod_{f \in \mathcal{F}_G} \mathfrak{X}_{(f)}$. Observando fenômeno análogo para operadores do tipo $\mathfrak{Z}$, $\mathfrak{Z}_{(f)}$, tem-se que a quantidade de geradores independentes do grupo estabilizador é $2(\#\mathcal{F}_R + \#\mathcal{F}_B + \#\mathcal{F}_G) - 4$, assim, se k é quantidade de qubits lógicos do código, temos:

$$\begin{aligned}
k &= \#\mathcal{V} - (2(\#\mathcal{F}_R + \#\mathcal{F}_B + \#\mathcal{F}_G) - 4) && (3.1)\\
&= \frac{p\#\mathcal{F}}{3} - 2\#\mathcal{F} + 4 && (3.2)\\
&= \frac{p\#\mathcal{F} - 6\#\mathcal{F}}{3} + 4 && (3.3)\\
&= \frac{(p-6)\#\mathcal{F}}{3} + 4 && (3.4)\\
&= \frac{1}{3}(p-6)\frac{12(g-1)}{p-6} + 4 && (3.5)\\
&= 4(g-1) + 4 && (3.6)\\
&= 4g. && (3.7)
\end{aligned}$$

Portanto, embora o comprimento do código colorido seja eventualmente maior do que o do código de superfície obtido da mesma tesselação, este codifica o dobro de qubits lógicos.

Observação 3.8.1. Uma tesselação regular 3-colorível é composta apenas por polígonos cuja quantidade de lados é par, conforme explanado em [50].

Exemplo 3.8.2. Código colorido $[16, 8, 2]$ de [50], obtido da tesselação $\{8, 3\}$ sobre o 2-toro.

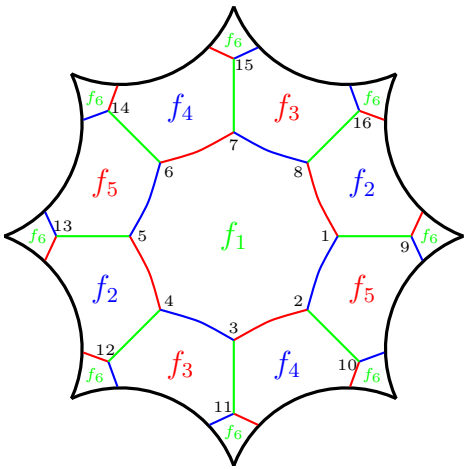


Figura 3.9: Tesselação regular $\{8, 3\}$ sobre o 2-toro, da qual se extrai o código quântico colorido $[16, 8, 2]$. Os (16) qubits físicos estão enumerados de 1 a 16, as arestas estão coloridas conforme um padrão de escolha predeterminado e a etiqueta de cada uma das 6 faces está grafada na cor correspondente da face, nesta construção.

Os operadores face deste código são:

$$\mathfrak{X}_{(f_1)} = \mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_8 \qquad \mathfrak{Z}_{(f_1)} = \mathfrak{Z}_3\mathfrak{Z}_4\mathfrak{Z}_5\mathfrak{Z}_6\mathfrak{Z}_7\mathfrak{Z}_8$$

$$\mathfrak{X}_{(f_2)} = \mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_8\mathfrak{X}_9\mathfrak{X}_{12}\mathfrak{X}_{13}\mathfrak{X}_{16} \qquad \mathfrak{Z}_{(f_2)} = \mathfrak{Z}_4\mathfrak{Z}_5\mathfrak{Z}_8\mathfrak{Z}_9\mathfrak{Z}_{12}\mathfrak{Z}_{13}\mathfrak{Z}_{16}$$

$$\mathfrak{X}_{(f_3)} = \mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_7\mathfrak{X}_8\mathfrak{X}_{11}\mathfrak{X}_{12}\mathfrak{X}_{15}\mathfrak{X}_{16} \qquad \mathfrak{Z}_{(f_3)} = \mathfrak{Z}_3\mathfrak{Z}_4\mathfrak{Z}_7\mathfrak{Z}_8\mathfrak{Z}_{11}\mathfrak{Z}_{12}\mathfrak{Z}_{15}\mathfrak{Z}_{16}$$

$$\mathfrak{X}_{(f_4)} = \mathfrak{X}_3\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_{10}\mathfrak{X}_{11}\mathfrak{X}_{14}\mathfrak{X}_{15} \qquad \mathfrak{Z}_{(f_4)} = \mathfrak{Z}_3\mathfrak{Z}_6\mathfrak{Z}_7\mathfrak{Z}_{10}\mathfrak{Z}_{11}\mathfrak{Z}_{14}\mathfrak{Z}_{15}$$

$$\mathfrak{X}_{(f_5)} = \mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_9\mathfrak{X}_{10}\mathfrak{X}_{13}\mathfrak{X}_{14} \qquad \mathfrak{Z}_{(f_5)} = \mathfrak{Z}_5\mathfrak{Z}_6\mathfrak{Z}_9\mathfrak{Z}_{10}\mathfrak{Z}_{13}\mathfrak{Z}_{14}$$

$$\mathfrak{X}_{(f_6)} = \mathfrak{X}_9\mathfrak{X}_{10}\mathfrak{X}_{11}\mathfrak{X}_{12}\mathfrak{X}_{13}\mathfrak{X}_{14}\mathfrak{X}_{15}\mathfrak{X}_{16} \qquad \mathfrak{Z}_{(f_6)} = \mathfrak{Z}_9\mathfrak{Z}_{10}\mathfrak{Z}_{11}\mathfrak{Z}_{12}\mathfrak{Z}_{13}\mathfrak{Z}_{14}\mathfrak{Z}_{15}\mathfrak{Z}_{16}$$

Os operadores provenientes das faces f_5 e f_6 são gerados pelos demais quatro operadores, a saber, tomando-se $A \in \{\mathfrak{X}, \mathfrak{Z}\}$, tem-se $A_{(f_5)} = A_{(f_1)}A_{(f_2)}A_{(f_4)}$ e $A_{(f_6)} = A_{(f_2)}A_{(f_3)}A_{(f_4)}$.

Tesselações Reduzidas e os Operadores String

Uma tesselação reduzida proveniente de uma tesselação 3-valente e 3-colorível pode ser facilmente compreendida por meio da linguagem de grafos. A tesselação reduzida de cada uma das três cores é, em síntese, o grafo desconexo obtido ao desconsiderar-se as arestas das demais duas cores. Para fins do nosso estudo, podemos interpretar a rede reduzida vermelha, por exemplo, como sendo o grafo obtido ao se desconsiderar qualquer aresta verde ou azul e, adicionalmente, para cada face vermelha, adicionar arestas conectando todos os pares de vértices. Estas arestas adicionais são auxiliares e jamais vão representar a atuação

de qualquer operador de Pauli, isto é, os operadores de Pauli atuam apenas sobre as arestas da tesselação original. Esta forma de interpretar uma rede reduzida é bastante conveniente pois nos fornece uma maneira prática de aferir o colchete de dois operadores, dados por uma decomposição especifica, a qual é explanada mais abaixo.

Seja $\rho \in \{R, G, B\}$, $\gamma \in \mathfrak{Z}_1$ um ciclo qualquer e $\mathcal{V}^{\rho}_{(\gamma)}$ o conjunto dos vértices de γ situados sobre arestas associadas à cor ρ. Existem 6 operadores associados ao par (γ, ρ):

$$\mathfrak{X}^{\rho}_{(\gamma)} = \prod_{v \in \mathcal{V}^{\rho}_{(\gamma)}} \mathfrak{X}_{(v)}, \quad \mathfrak{Z}^{\rho}_{(\gamma)} = \prod_{v \in \mathcal{V}^{\rho}_{(\gamma)}} \mathfrak{Z}_{(v)}$$

Estes operadores são chamados de Operadores String e possuem uma característica interessante aos códigos quânticos coloridos: Dois operadores String de mesma cor (R, G ou B) ou do mesmo tipo ($\mathfrak{X}$ ou $\mathfrak{Z}$) sempre comutam. Desta forma, duas strings anticomutam se, e só se, possuem cor e tipo distintos, simultaneamente.

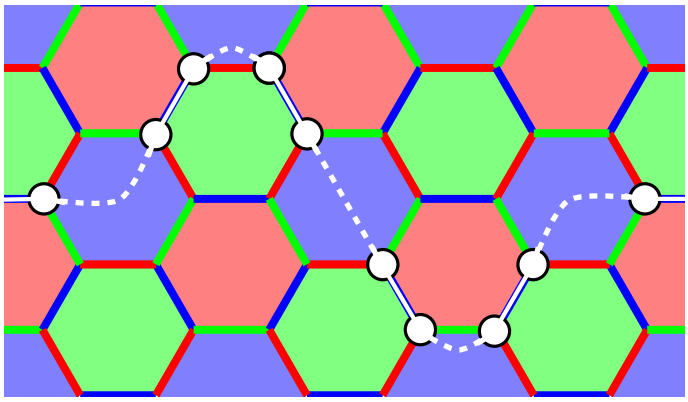


Figura 3.10: Operador string azul, com seu suporte em destaque.

Sendo $\partial(\gamma) = 0$, segue que $\mathfrak{X}^{R}_{(\gamma)}\mathfrak{X}^{G}_{(\gamma)}\mathfrak{X}^{B}_{(\gamma)} = \mathfrak{Z}^{R}_{(\gamma)}\mathfrak{Z}^{G}_{(\gamma)}\mathfrak{Z}^{B}_{(\gamma)} = Id$, de onde verifica-se que uma das cores é dependente das outras duas. Portanto, pode-se considerar apenas duas dentre as três cores (e.g. R e G).

Um operador string de uma determinada cor, a qual sem perder generalidade, podemos supor azul, pode eventualmente bifurcar em dois operadores string, cada um destes com uma das duas cores restantes e, eventualmente, colapsar para prosseguir como um operador string. Este tipo de operador string comumente é chamado de Operador T-String.

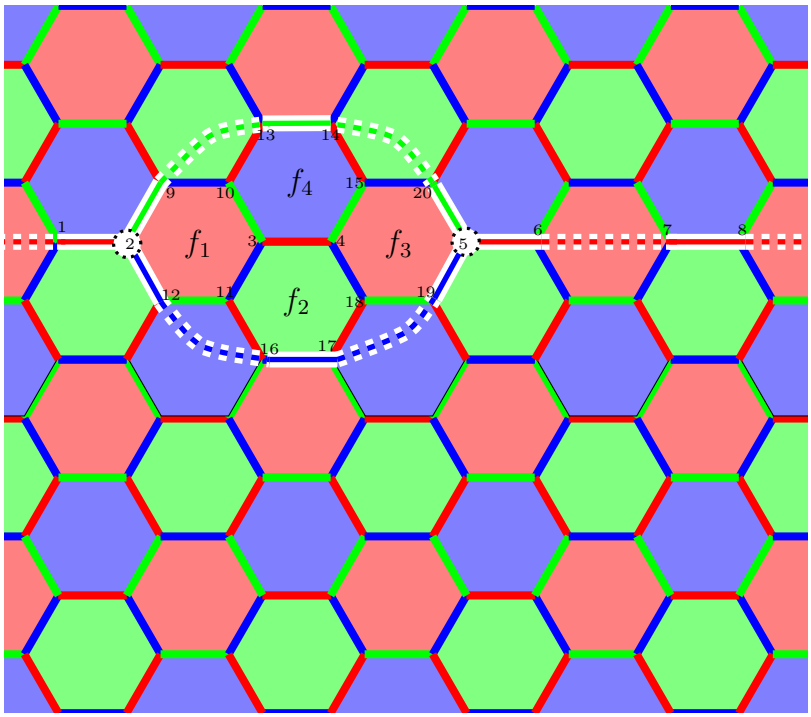


Figura 3.11: Um operador string vermelho bifurcando em dois operadores, um verde e outro azul, os quais colapsam novamente, dando continuidade a um segmento de cadeia que está relacionada a um operador vermelho, [50]. Esta T-string é obtida pelo produto do operador string inicial, $\mathfrak{X}_1\mathfrak{X}_2\mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_8$, com os operadores face azuis relacionados às faces $f_1, \cdots, f_4$, envoltas pela T-string resultante. Esta T-string resulta ser o operador $\mathfrak{X}_1\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_8\mathfrak{X}_9\mathfrak{X}_{12}\mathfrak{X}_{13}\mathfrak{X}_{14}\mathfrak{X}_{16}\mathfrak{X}_{17}\mathfrak{X}_{19}\mathfrak{X}_{20}$. Vale observar que esta t-string não atua nos qubits destacados, a saber, 2 e 5.

Observação 3.8.3. Uma condição necessária para que uma tesselação $\{p, 3\}$ seja 3-colorível é que a sua quantidade de faces seja divisível por 3.

Para justificar esta afirmação, considere uma tesselação regular do g-toro, 3-valente e 3-colorível $\{p, 3\}$, onde $g \geq 2$. Sejam $\#\mathcal{V}$, $\#\mathcal{E}$ e $\#\mathcal{F}$ as quantidades de vértices, arestas e faces desta, respectivamente. Adicionalmente, sejam $\#\mathcal{E}(C)$ e $\#\mathcal{F}(C)$ a quantidade de arestas e faces de cor $C \in \{R, G, B\}$, respectivamente.

Fixada uma cor $C_1 \in \{R, G, B\}$, nota-se que de cada vértice emana, com esta mesma cor fixada, exatamente uma aresta, a qual é comum a algum outro vértice da tesselação. Desta forma, $\#\mathcal{E}(C_1) = \#\mathcal{V}/2$ e, como $2\#\mathcal{E} = 3\#\mathcal{V} = p\#\mathcal{F}$, segue que $\#\mathcal{E}(C_1) = \frac{p\#\mathcal{F}}{6}$. Ainda, como uma aresta da cor C_1 pertence simultaneamente a uma face de cor C_2 e uma face de cor C_3, com $C_i \neq C_j$ sempre que $i \neq j$, segue que $\frac{p\#\mathcal{F}}{6} = \#\mathcal{E}(C_1) = \frac{\frac{p\#\mathcal{F}(C_2)}{2} + \frac{p\#\mathcal{F}(C_3)}{2}}{2} = \frac{p\#\mathcal{F}(C_2)+p\#\mathcal{F}(C_3)}{4}$, de onde segue que $2\#\mathcal{F} = 3\left(\#\mathcal{F}(C_2) + \#\mathcal{F}(C_3)\right)$ de onde podemos concluir que 3 divide $\#\mathcal{F}$.

Observação 3.8.4. A tesselação reduzida de qualquer cor é a tesselação regular $\{p/2, p\}$.

Fixada, sem perda de generalidade, a cor vermelha da tesselação $\{p, 3\}$, nota-se que cada face de cor azul ou verde dá lugar, ao passar para a tesselação reduzida vermelha, à uma face com quantidade de arestas igual à $p/2$. As arestas da tesselação reduzida são constituídas pelo prolongamento das arestas de cor vermelha da tesselação original, até o incentro das faces vermelhas. Como sabe-se, emanam p arestas vermelhas de cada face vermelha, portanto, a tesselação reduzida possui vértices de valência p.

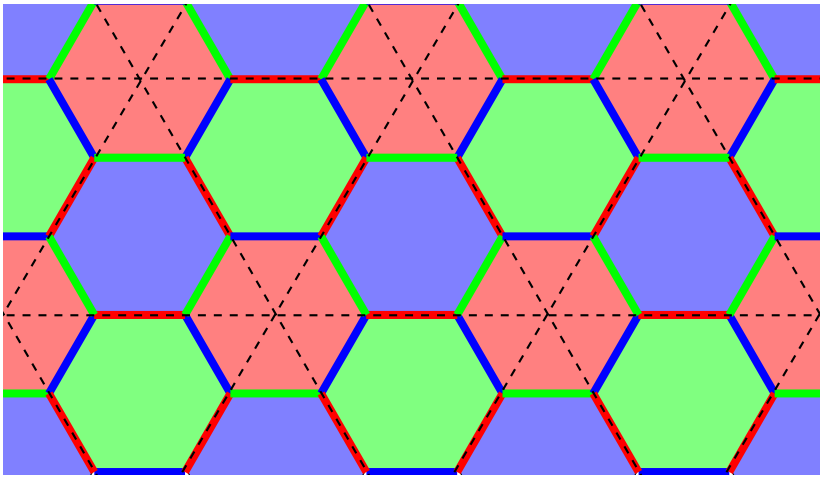


Figura 3.12: As arestas pontilhadas configuram a tesselação reduzida vermelha, proveniente da tesselação $\{p, 3\}$. Esta é a tesselação $\{p/2, p\}$: Cada vértice situado no incentro de uma face da cor relativa tem valência p, enquanto que apenas metade das arestas das demais faces da tesselação original, ao serem prolongadas até o incentro das faces da cor relativa, passam determinam uma aresta da tesselação reduzida.

Considerando que no âmbito da geometria hiperbólica não existe a noção de semelhança entre polígonos, segue que os polígonos das tesselações reduzidas das três cores são congruentes e, portanto [3], estão em quantidades iguais. Isto reforça o estabelecido na observação 3.8.3.

Distância Mínima de um Código Quântico Colorido

Tendo em vista que um código colorido é, em particular, um código estabilizador, segue que sua distância mínima é o menor peso dentre todos os possíveis representantes de seus operadores lógicos, isto é, o menor peso dentre os elementos de $\mathcal{N}(\mathcal{S}_{est}) - \mathcal{S}_{est}$, onde $\mathcal{S}_{est}$ é

[3] A quantidade de faces de uma cor específica é exatamente igual à quantidade de vértices da tesselação $\{p/2, p\}$, quando esta se encontra tesselando o g-toro

o grupo estabilizador que o determina. Por conta da construção peculiar em detrimento dos códigos de superfície, um operador lógico de um código colorido não necessariamente é determinado por um ciclo de homologia não trivial, em se tratando da homologia da superfície e da tesselação subjacentes à construção deste. Podemos ilustrar esta situação com os dados obtidos no exemplo 3.8.2. Veja abaixo:

Exemplo 3.8.5. Note que no exemplo 3.8.2, o menor ciclo de homologia não trivial atua sobre 4 qubits, fato qual pode induzir à inferência de que a distância mínima é 4, fazendo-se um paralelo com os códigos de superfície. Porém, lembrando que a distância do código é obtida do peso do operador lógico de menor peso, basta notar que, por exemplo, os operadores $\mathfrak{X}_s\mathfrak{X}_{s+4}$, $\mathfrak{Z}_s\mathfrak{Z}_{s+4}$, onde $s \in \{1, \cdots, 4, 9, \cdots, 12\}$, são operadores lógicos de peso 2.

Devido a construção do código, podemos afirmar que um operador lógico deve ter peso par, segue que estes acima fornecem a distância do código.

Esta anomalia, de um operador determinado por uma string que não é um ciclo ser um operador lógico, ocorre devido ao fato de a tesselação possuir pelo menos um par de faces que possuem mais de uma aresta em comum, como é o caso das faces f_2 e f_5 que possuem em comum as arestas determinadas pelos vértices 1 e 9, e 5 e 13, respectivamente.

Proposição 3.8.6. A distância de um código quântico colorido proveniente de uma tesselação regular do g-toro, $g \geq 2$, que possui exatamente 3 faces é igual a 2.

Demonstração: Fixada uma face e tomando-se um vértice v_1 desta, tem-se que a aresta que dela emana, a partir de v_1, acaba tendo sua outra extremidade noutro vértice, digamos v_2, desta mesma face. Não é difícil perceber que v_1 e v_2 são dois vértices distintos que pertencem, simultaneamente, a todas as três faces da tesselação. O operador $A_{(v_1)}A_{(v_2)}$, $A \in \{\mathfrak{X}, \mathfrak{Z}\}$ é, portanto, um operador lógico deste código. □

Proposição 3.8.7. A distância de um código quântico colorido proveniente de uma tesselação regular do g-toro, $g \geq 2$, que possui exatamente 6 faces é igual a 2. Demonstração: Se $\{p, 3\}$ é uma tesselação do g-toro com 6 faces, tem-se $\dfrac{12(g-1)}{p-6} = 6$, de onde segue que $p = 2g + 4$. Como $g \geq 2$, tem-se $p \geq 8$.

Sejam $f_1, \cdots, f_6$ os rótulos de tais faces, as quais a menos de um reordenamento nos índices, podemos supor f_1 e f_6 serem verdes, f_2 e f_4 azuis e f_3 e f_5 vermelhas. Sejam

$v_1, \cdots, v_p$ os vértices de f_1, enumerados de forma circular e que e_i é a aresta que emana da face f_1 a partir do vértice v_i, para cada $i = 1, \cdots, j \leq p$, onde j é a quantidade de arestas distintas que emanam de f_1. A igualdade de j e p se dá somente quando todas as arestas e_i possuem um extremo em um vértice que não pertence a f_1.

Caso 1. Se $p > j$, a distância do código quântico colorido subjacente à esta tesselação é 2.

De fato, sendo $p > j$, existe um índice i, para o qual e_i possui as duas extremidades sobre vértices de f_1. Sejam, a menos de um reordenamento, v_1 e v_i tais vértices, enquanto que as duas faces que determinam e_1 são f_2 e f_3. A figura 3.13 ilustra esta situação.

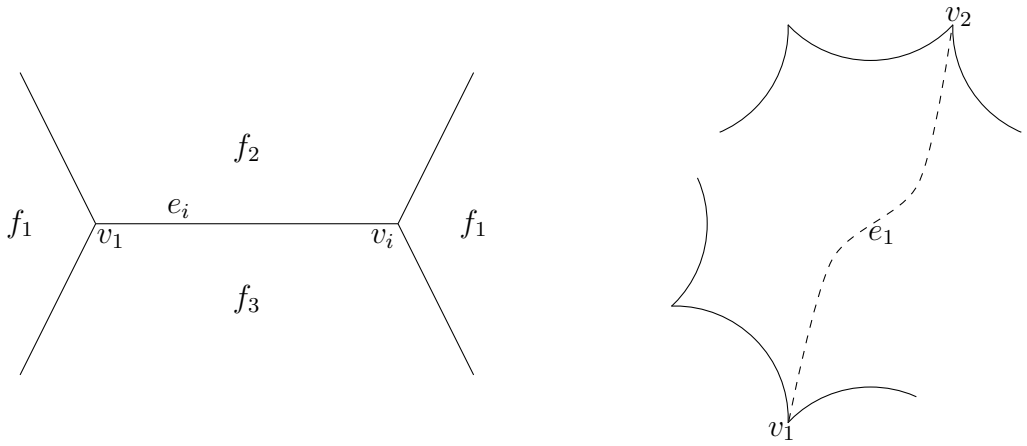


Figura 3.13: Uma aresta e_i, determinada pelos vértices v_1 e v_i, ambos situados sobre uma mesma face f_1. As faces f_2 e f_3 possuem e_i em seu bordo.

Desta forma, os vértices v_1 e v_α pertencem única e simultaneamente às faces f_1, f_2 e f_3. Com isto, dado $A \in \{\mathfrak{X}_{(\gamma)}, \mathfrak{Z}\}$, tem-se $A_{(v_1)}A_{(v_\alpha)} \in \mathcal{N}(\mathcal{S}_{est})$.

Caso 2. Se $p = j$, a distância do código quântico colorido subjacente à esta tesselação é 2.

Para garantir a validade desta afirmação, atribua para cada $i = 1, \cdots, p \in \mathbb{Z}_p$, o símbolo $e(i, i+1)$ para a aresta da face f_1 cujos extremos são os vértices v_i e v_{i+1}. Suponha que $e(1, 2)$ é uma aresta da face f_2 e que $e(2, 3)$ é aresta da face f_3.

Se $e(3, 4)$ é uma aresta de f_2, tem-se $A_{(v_2)}A_{(v_3)} \in \mathcal{N}(\mathcal{S}_{est})$, para cada $A \in \{\mathfrak{X}, \mathfrak{Z}\}$. Agora, se $e(3, 4)$ não é aresta da face f_2, então é aresta da face f_4.

Se $e(4, 5)$ é uma aresta da face f_3, tem-se $A_{(v_3)}A_{(v_4)} \in \mathcal{N}(\mathcal{S}_{est})$, para cada $A \in \{\mathfrak{X}, \mathfrak{Z}\}$. Se não, $e(4, 5)$ é aresta da face f_5.

Se $e(5,6)$ é uma aresta da face f_4, segue que $A_{(v_4)}A_{(v_5)} \in \mathcal{N}(\mathcal{S}_{est})$, para cada $A \in \{\mathfrak{X}, \mathfrak{Z}\}$. Caso contrário, $e(5,6)$ é uma aresta de f_2.

Se $e(6,7)$ é uma aresta da face f_5, segue que $A_{(v_6)}A_{(v_7)} \in \mathcal{N}(\mathcal{S}_{est})$, para cada $A \in \{\mathfrak{X}, \mathfrak{Z}\}$. Caso $e(6,7)$ não seja uma aresta da face f_5, então é aresta da face f_3. Nesta ocasião, os vértices v_2 e v_6 pertencem única e simultaneamente às faces f_1, f_2 e f_3. Assim sendo, tem-se $A_{(v_2)}A_{(v_3)} \in \mathcal{N}(\mathcal{S}_{est})$, para cada $A \in \{\mathfrak{X}, \mathfrak{Z}\}$.□

O que as proposições 3.8.6 e 3.8.7 tem em comum é que ambas tratam de um caso particular de algo ligeiramente mais geral: As tesselações ali empregadas tem a característica de ter em comum a pelo menos uma terna de faces de cores distintas, um par de vértices distintos. O operador que atua com uma mesma matriz de Pauli nos qubits relacionados a tais vértices comuta com os geradores do grupo estabilizador e portanto, pertence ao normalizador de tal. Obviamente, se a matriz empregada for a matriz $\mathfrak{X}$, por exemplo, o operador resultante é um operador lógico com suporte em exatamente dois qubits, garantido assim que a distância do código subjacente é 2.

Uma maneira prática de identificarmos algumas das tesselações de valência 3, que são 3-coloríveis, que venham a fornecer códigos de distância 2 é observando se a quantidade de ternas de 3 faces de cores distintas entre sí é, ou não, menor do que a quantidade de vértices desta tesselação. Se a quantidade destas ternas é menor do que a quantidade de vértices, obrigatoriamente haverá pelo menos um par de vértices sobre uma mesma terna e, devido à construção dos códigos coloridos e pelo fato desta tesselação ter valência 3, ter-se-á um operador lógico com suporte em dois qubits.

Caso ocorra de a quantidade de ternas de 3 faces de cores distintas entre sí não ser menor do que a quantidade de vértices desta tesselação, este método nada conclui sobre a mesma, induzindo a outro tipo de análise.

O método supracitado consiste em notar que se uma tesselação tem $\#\mathcal{F}$ faces, ter-se-á $\dfrac{\#\mathcal{F}}{3}$ faces de cada uma das três cores. A quantidade de ternas de faces de cores distintas entre sí não é maior, portanto, do que $\left(\dfrac{\#\mathcal{F}}{3}\right)^3$. Já a quantidade de vértices é dada por $\mathcal{V} = \dfrac{p\#\mathcal{F}}{3}$. Com um cálculo simples se garante que nos casos em que a tesselação possui 3, 6

ou 9 faces, a distância do código subjacente vai ser 2, independentemente de $g \geq 2$ escolhido.

Exemplo 3.8.8. Fixado um inteiro positivo m, escolha um inteiro par $p > 16m^2$ e defina $g = pm - 6m + 1$. Se a tesselação $\{p, 3\}$ sobre o g-toro for 3-colorível, o código colorido subjacente tem distância 2. De fato, esta tessela o g-toro com $12m$ faces e $4pm$ vértices. A quantidade de ternas de faces de cores distintas não é maior do que $\left(\frac{12m}{3}\right)^3 = 64m^3$. Como $16m^2 < p$, tem-se $64m^3 < 4pm$ e, portanto, o código colorido subjacente tem distância 2.

Na mesma linha de raciocínio, considere $\{p, 3\}$ uma tesselação regular 3-colorível do g-toro, $g \geq 2$. Fixada uma face f_1, de cor verde por exemplo, desta emanam p arestas verdes. Cada uma destas arestas verdes possuem a outra extremidade num vértice de alguma face verde, a qual eventualmente pode ser a face f_1. Caso ocorra de a aresta possuir as duas extremidades sobre uma mesma face, com um argumento análogo ao exposto na observação 3.8.3 garante-se que a distância do código colorido subjacente a tal tesselação é 2.

Agora, se apenas as arestas de f_1 possuem mais do que um vértice sobre esta face, pode ocorrer a situação de que duas arestas que emanam de f_1 tenham a outra extremidade numa mesma face f_α, distinta de f_1. A menos de um reordenamento, podemos supor que uma destas arestas tem como vértices $v_1 \in f_1$ e $v_1' \in f_\alpha$ enquanto que a outra aresta tem como vértices $v_j \in f_1$ e $v_j' \in f_\alpha$. Neste caso, o operador $\mathfrak{X}_{(v_1)}\mathfrak{X}_{(v_1')}\mathfrak{X}_{(v_j)}\mathfrak{X}_{(v_j')}$ pertence ao normalizador do grupo estabilizador do código subjacente à tesselação. Para garantir que este não pertence ao grupo estabilizador, basta notar que, passando à tesselação reduzida verde, a string que o determina é composta por dois arcos de geodésica, conectando os incentros de f_1 e f_α.

A prova da proposição que segue é baseada no argumento acima.

Proposição 3.8.9. Se $\{p, 3\}$ é uma tesselação 3-colorível, tal que $\frac{\#\mathcal{F}}{3} - 1 < p$, então a distância do código colorido subjacente à está tem distância não maior do que 4.

Observação 3.8.10. Tem-se $\frac{\#\mathcal{F}}{3} - 1 < p$ se, e somente se[4], $4g < p^2 - 5p - 2$.

Exemplo 3.8.11. Segue abaixo uma tabela com tesselações $\{p, 3\}$ do g-toro cuja distância não é maior do que 4, segundo a observação 3.8.10.

[4]Lembre que $\#\mathcal{F} = \frac{12(g-1)}{p-6}$

p \ g	2	3	4	5	6	7	8	9	10	11	12	13
8		⋆	⋆	⋆								
10				⋆	⋆	⋆	⋆	⋆	⋆	⋆		
12	⋆	⋆		⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆	⋆
14								⋆		⋆		⋆
16										⋆		
18	⋆	⋆		⋆	⋆		⋆	⋆		⋆	⋆	⋆
20												
22												
24			⋆			⋆						⋆
26												
28												
30		⋆		⋆				⋆		⋆		
32												
34												
36					⋆					⋆		
38												
40												
42			⋆			⋆						⋆

Proposição 3.8.12. Se $\{p, q\}$ é uma tesselação regular 3-valente e 3-colorível do g-toro, com $g \geq 2$, então:

i. Se alguma aresta de uma de suas tesselações reduzidas é um loop sobre algum vértice, então a distância do código colorido subjacente é igual a 2;

ii. Se existem pelo menos duas arestas distintas de uma de suas tesselações reduzidas que possuam o mesmo bordo, então a distância do código colorido subjacente não é maior do que 4;

iii. Se a quantidade de arestas de qualquer tesselação reduzida é igual a p, então a distância do código colorido subjacente não é maior do que 4;

iv. Se a quantidade de arestas de qualquer tesselação reduzida é menor do que p, então a distância do código colorido subjacente é igual a 2.

Demonstração: i: A existência de um loop na tesselação reduzida está condicionada à existência de uma aresta da tesselação original, cujos dois vértices que constituem o bordo pertencem à uma mesma face, enquanto que o bordo de tal face não contém a referida aresta. O operador que atua com $\mathfrak{X}$ sobre os dois qubits relacionados a estes dois vértices é um operador lógico.

ii: Se tais arestas, digamos e_1 e e_2, são loops, estão satisfeitas as hipóteses do item i. Caso contrário, existem vértices $v_1 \neq v_2$ da tesselação reduzida, tais que $\partial(e_i) = \{v_1, v_2\}$. Sejam f_i as faces da tesselação original cujo incentro é v_i. Como e_i não é um loop, tem-se

$f_1 \neq f_2$. Seja e_i' a aresta da tesselação original cuja extensão fornece a aresta e_i da tesselação reduzida. Sejam $\partial(e_i') = \{v_a, v_b\}$ e $\partial(e_2') = \{v_c, v_d\}$. O operador $\mathfrak{X}_{v_a}\mathfrak{X}_{v_b}\mathfrak{X}_{v_c}\mathfrak{X}_{v_d}$ é lógico.

iii: Note que p é a valência de cada vértice da tesselação reduzida. Ou uma aresta é um loop sobre algum vértice, ou obrigatoriamente existem duas arestas distintas cujo bordo comum, satisfazendo as hipóteses do item ii.

iv: Sendo p a valência de qualquer vértice da tesselação reduzida, de cada vértice v desta emanam p arestas. Como a tesselação reduzida consta de menos arestas do que p, por hipótese, seque que ao menos uma aresta caracteriza um loop sobre v, satisfazendo as hipóteses do item i. □

Exemplo 3.8.13. Se $p > 2g+4$, a distância do código colorido subjacente à tesselação $\{p, 3\}$ sobre o g-toro, $g \geq 2$, é igual a 2.

De fato, percebendo-se que a quantidade de faces de uma das tesselações reduzidas é igual a $\frac{p.\#\mathcal{F}}{6}$, onde $\mathcal{F}$ é o conjunto das faces da tesselação $\{p, 3\}$, com um simples cálculo garante-se que, se $p > 2g + 4$, então p supera a quantidade de arestas desta tesselação reduzida. A proposição 3.8.12 garante o restante deste argumento.

Capítulo 4

Novos Códigos Quânticos de Superfície

4.1 Novos Códigos de Superfície

Neste capítulo estudaremos os códigos de superfície obtidos por tesselações semirregulares.

A partir das tesselações derivadas, estudadas na seção 1.5.3, constrói-se os códigos de superfície da seção 4.1.1.

4.1.1 Códigos de Superfície Provenientes das Tesselações Semirregulares $[p,q,p,q]$, $[2p,2p,q]$ e $[2p,2q,4]$ do g-toro

Como introdução aos resultados da presente tese, apresentamos abaixo três famílias de códigos de superfície provenientes das tesselações derivadas.

Códigos de Superfície Provenientes de Tesselações $[p,q,p,q]$ do g-toro, $g \geq 2$: O código quântico de superfície obtido a partir da tesselação semirregular $[p,q,p,q]$ situada sobre o g-toro, $g \geq 2$, derivada da tesselação regular $\{p,q\}$, é composto por $n = \dfrac{4pq(g-1)}{pq-2p-2q}$ qubits físicos, $k = 2g$ qubits lógicos e um limitante inferior para a distância deste é obtido pelo menor inteiro, não menor do que o mínimo do conjunto $\left\{\dfrac{d_{\mathbb{M}}}{L}, \dfrac{d_{\mathbb{M}}}{r}\right\}$, onde L é o comprimento de aresta da tesselação $[p,q,p,q]$, e r é o comprimento do raio da circunferência circunscrita a um p- gon da tesselação regular $\{p,q\}$.

Seguem abaixo algumas tabelas com os parâmetros de alguns dos códigos assim obtidos.

#	g	Tesselação	$[n, k, d]$
1	2	[3,7,3,7]	$[84, 4, 5]$
2	2	[3,8,3,8]	$[48, 4, 4]$
3	2	[3,9,3,9]	$[36, 4, 3]$
4	2	[3,10,3,10]	$[30, 4, 3]$
5	2	[3,12,3,12]	$[24, 4, 3]$
6	2	[4,5,4,5]	$[40, 4, 4]$
7	2	[4,6,4,6]	$[24, 4, 3]$
8	2	[4,8,4,8]	$[16, 4, 2]$
9	2	[4,12,4,12]	$[12, 4, 2]$
10	2	[5,5,5,5]	$[20, 4, 3]$
11	2	[5,10,5,10]	$[10, 4, 2]$
12	2	[6,6,6,6]	$[12, 4, 2]$
13	2	[8,8,8,8]	$[8, 4, 2]$

#	g	Tesselação	$[n, k, d]$
14	3	[3,7,3,7]	$[168, 6, 7]$
15	3	[3,8,3,8]	$[96, 6, 5]$
16	3	[3,9,3,9]	$[72, 6, 4]$
17	3	[3,10,3,10]	$[60, 6, 4]$
18	3	[3,12,3,12]	$[48, 6, 3]$
19	3	[4,5,4,5]	$[80, 6, 5]$
20	3	[4,6,4,6]	$[48, 6, 4]$
21	3	[4,8,4,8]	$[32, 6, 3]$
22	3	[4,12,4,12]	$[24, 6, 2]$
23	3	[5,5,5,5]	$[40, 6, 4]$
24	3	[5,6,5,6]	$[30, 6, 3]$
25	3	[5,10,5,10]	$[20, 6, 2]$
26	3	[6,6,6,6]	$[24, 6, 3]$
27	3	[6,9,6,9]	$[18, 6, 2]$
28	3	[8,8,8,8]	$[16, 6, 2]$
29	3	[12,12,12,12]	$[12, 6, 2]$

#	g	Tesselação	$[n, k, d]$
30	4	[3,7,3,7]	$[252, 8, 8]$
31	4	[3,8,3,8]	$[144, 8, 6]$
32	4	[3,9,3,9]	$[108, 8, 5]$
33	4	[3,10,3,10]	$[90, 8, 4]$
34	4	[3,12,3,12]	$[72, 8, 4]$
35	4	[4,5,4,5]	$[120, 8, 6]$
36	4	[4,6,4,6]	$[72, 8, 5]$
37	4	[4,7,4,7]	$[56, 8, 4]$
38	4	[4,8,4,8]	$[48, 8, 4]$
39	4	[4,10,4,10]	$[40, 8, 3]$
40	4	[4,12,4,12]	$[36, 8, 3]$
41	4	[5,5,5,5]	$[60, 8, 4]$
42	4	[5,10,5,10]	$[30, 8, 3]$
43	4	[6,6,6,6]	$[36, 8, 3]$
44	4	[6,12,6,12]	$[24, 8, 2]$
45	4	[7,7,7,7]	$[28, 8, 3]$
46	4	[8,8,8,8]	$[24, 8, 2]$
47	4	[10,10,10,10]	$[20, 8, 2]$

#	g	Tesselação	$[n, k, d]$
48	5	[3,7,3,7]	$[336, 10, 9]$
49	5	[3,8,3,8]	$[192, 10, 6]$
50	5	[3,9,3,9]	$[144, 10, 5]$
51	5	[3,10,3,10]	$[120, 10, 5]$
52	5	[3,12,3,12]	$[96, 10, 4]$
53	5	[4,5,4,5]	$[160, 10, 7]$
54	5	[4,6,4,6]	$[96, 10, 5]$
55	5	[4,8,4,8]	$[64, 10, 4]$
56	5	[4,12,4,12]	$[48, 10, 3]$
57	5	[5,5,5,5]	$[80, 10, 5]$
58	5	[5,6,5,6]	$[60, 10, 4]$
59	5	[5,10,5,10]	$[40, 10, 3]$
60	5	[6,6,6,6]	$[48, 10, 3]$
61	5	[6,7,6,7]	$[42, 10, 3]$
62	5	[6,9,6,9]	$[36, 10, 3]$
63	5	[8,8,8,8]	$[32, 10, 3]$
64	5	[12,12,12,12]	$[24, 10, 2]$

Códigos de Superfície Provenientes de Tesselações $[2p, 2p, q]$ do g-toro, $g \geq 2$: O código quântico de superfície obtido a partir da tesselação semirregular $[2p, 2p, q]$ situada

sobre o g-toro, $g \geq 2$, derivada da tesselação regular $\{p, q\}$, é composto por $n = \dfrac{6pq(g-1)}{pq-2p-2q}$ qubits físicos, $k = 2g$ qubits lógicos e um limitante inferior para a distância deste é obtido pelo menor inteiro, não menor do que o mínimo do conjunto $\left\{\dfrac{d_{\mathbb{M}}}{L}, \dfrac{d_{\mathbb{M}}}{2a}, \dfrac{d_{\mathbb{M}}}{r}\right\}$, onde L é o comprimento de aresta da tesselação $[2p, 2p, q]$ e a e r são, respectivamente, o comprimento do apótema e do raio de um polígono da tesselação regular $\{p, q\}$.

Seguem abaixo algumas tabelas com os parâmetros de alguns dos códigos assim obtidos.

#	g	Tesselação	$[n, k, d]$
1	2	[14,14,3]	$[126, 4, 3]$
2	2	[16,16,3]	$[72, 4, 2]$
3	2	[18,18,3]	$[54, 4, 2]$
4	2	[20,20,3]	$[45, 4, 2]$
5	2	[24,24,3]	$[36, 4, 2]$
6	2	[36,36,3]	$[27, 4, 1]$
7	2	[10,10,4]	$[60, 4, 3]$
8	2	[12,12,4]	$[36, 4, 2]$
9	2	[16,16,4]	$[24, 4, 2]$
10	2	[24,24,4]	$[18, 4, 1]$
11	2	[8,8,5]	$[60, 4, 3]$
12	2	[10,10,5]	$[30, 4, 2]$
13	2	[20,20,5]	$[15, 4, 1]$
14	2	[8,8,6]	$[36, 4, 3]$
15	2	[12,12,6]	$[18, 4, 2]$
16	2	[6,6,7]	$[126, 4, 5]$
17	2	[6,6,8]	$[72, 4, 4]$
18	2	[8,8,8]	$[24, 4, 2]$
19	2	[16,16,8]	$[12, 4, 1]$
20	2	[6,6,9]	$[54, 4, 3]$
21	2	[6,6,10]	$[45, 4, 3]$
22	2	[10,10,10]	$[15, 4, 2]$
23	2	[6,6,12]	$[36, 4, 3]$
24	2	[8,8,12]	$[18, 4, 2]$
25	2	[6,6,18]	$[27, 4, 2]$

#	g	Tesselação	$[n, k, d]$
26	3	[14,14,3]	$[252, 6, 4]$
27	3	[16,16,3]	$[144, 6, 3]$
28	3	[18,18,3]	$[108, 6, 3]$
29	3	[20,20,3]	$[90, 6, 2]$

#	g	Tesselação	$[n, k, d]$
30	3	[24,24,3]	$[72, 6, 2]$
31	3	[28,28,3]	$[63, 6, 2]$
32	3	[36,36,3]	$[54, 6, 2]$
33	3	[10,10,4]	$[120, 6, 4]$
34	3	[12,12,4]	$[72, 6, 3]$
35	3	[16,16,4]	$[48, 6, 2]$
36	3	[24,24,4]	$[36, 6, 2]$
37	3	[40,40,4]	$[30, 6, 1]$
38	3	[8,8,5]	$[120, 6, 4]$
39	3	[10,10,5]	$[60, 6, 3]$
40	3	[12,12,5]	$[45, 6, 2]$
41	3	[20,20,5]	$[30, 6, 2]$
42	3	[8,8,6]	$[72, 6, 4]$
43	3	[10,10,6]	$[45, 6, 3]$
44	3	[12,12,6]	$[36, 6, 2]$
45	3	[18,18,6]	$[27, 6, 2]$
46	3	[6,6,7]	$[252, 6, 7]$
47	3	[28,28,7]	$[21, 6, 1]$
48	3	[6,6,8]	$[144, 6, 5]$
49	3	[8,8,8]	$[48, 6, 3]$
50	3	[16,16,8]	$[24, 6, 2]$
51	3	[6,6,9]	$[108, 6, 4]$
52	3	[12,12,9]	$[27, 6, 2]$
53	3	[6,6,10]	$[90, 6, 4]$
54	3	[10,10,10]	$[30, 6, 2]$
55	3	[6,6,12]	$[72, 6, 3]$
56	3	[8,8,12]	$[36, 6, 2]$
57	3	[24,24,12]	$[18, 6, 1]$
58	3	[6,6,14]	$[63, 6, 3]$
59	3	[14,14,14]	$[21, 6, 2]$
60	3	[6,6,18]	$[54, 6, 3]$
61	3	[8,8,20]	$[30, 6, 2]$

#	g	Tesselação	$[n, k, d]$
62	4	[14,14,3]	$[378, 8, 5]$
63	4	[16,16,3]	$[216, 8, 4]$
64	4	[18,18,3]	$[162, 8, 3]$
65	4	[20,20,3]	$[135, 8, 3]$
66	4	[24,24,3]	$[108, 8, 2]$
67	4	[30,30,3]	$[90, 8, 2]$
68	4	[36,36,3]	$[81, 8, 2]$
69	4	[10,10,4]	$[180, 8, 4]$
70	4	[12,12,4]	$[108, 8, 3]$
71	4	[14,14,4]	$[84, 8, 3]$
72	4	[16,16,4]	$[72, 8, 2]$
73	4	[20,20,4]	$[60, 8, 2]$
74	4	[24,24,4]	$[54, 8, 2]$
75	4	[32,32,4]	$[48, 8, 2]$
76	4	[8,8,5]	$[180, 8, 5]$
77	4	[10,10,5]	$[90, 8, 3]$
78	4	[20,20,5]	$[45, 8, 2]$
79	4	[8,8,6]	$[108, 8, 4]$
80	4	[12,12,6]	$[54, 8, 3]$
81	4	[24,24,6]	$[36, 8, 2]$
82	4	[6,6,7]	$[378, 8, 8]$
83	4	[8,8,7]	$[84, 8, 4]$
84	4	[14,14,7]	$[42, 8, 2]$
85	4	[6,6,8]	$[216, 8, 6]$
86	4	[8,8,8]	$[72, 8, 4]$
87	4	[16,16,8]	$[36, 8, 2]$
88	4	[6,6,9]	$[162, 8, 5]$
89	4	[36,36,9]	$[27, 8, 1]$
90	4	[6,6,10]	$[135, 8, 4]$
91	4	[8,8,10]	$[60, 8, 3]$
92	4	[10,10,10]	$[45, 8, 3]$
93	4	[20,20,10]	$[30, 8, 2]$
94	4	[6,6,12]	$[108, 8, 4]$
95	4	[8,8,12]	$[54, 8, 3]$
96	4	[12,12,12]	$[36, 8, 2]$
97	4	[6,6,15]	$[90, 8, 3]$
98	4	[8,8,16]	$[48, 8, 2]$
99	4	[32,32,16]	$[24, 8, 1]$
100	4	[6,6,18]	$[81, 8, 3]$
101	4	[18,18,18]	$[27, 8, 2]$

#	g	Tesselação	$[n, k, d]$
102	5	[14,14,3]	$[504, 10, 5]$
103	5	[16,16,3]	$[288, 10, 4]$
104	5	[18,18,3]	$[216, 10, 3]$
105	5	[20,20,3]	$[180, 10, 3]$
106	5	[24,24,3]	$[144, 10, 2]$
107	5	[28,28,3]	$[126, 10, 2]$
108	5	[36,36,3]	$[108, 10, 2]$
109	5	[10,10,4]	$[240, 10, 5]$
110	5	[12,12,4]	$[144, 10, 3]$
111	5	[16,16,4]	$[96, 10, 3]$
112	5	[24,24,4]	$[72, 10, 2]$
113	5	[40,40,4]	$[60, 10, 2]$
114	5	[8,8,5]	$[240, 10, 5]$
115	5	[10,10,5]	$[120, 10, 4]$
116	5	[12,12,5]	$[90, 10, 3]$
117	5	[20,20,5]	$[60, 10, 2]$
118	5	[8,8,6]	$[144, 10, 4]$
119	5	[10,10,6]	$[90, 10, 3]$
120	5	[12,12,6]	$[72, 10, 3]$
121	5	[14,14,6]	$[63, 10, 2]$
122	5	[18,18,6]	$[54, 10, 2]$
123	5	[30,30,6]	$[45, 10, 2]$
124	5	[6,6,7]	$[504, 10, 9]$
125	5	[12,12,7]	$[63, 10, 3]$
126	5	[28,28,7]	$[42, 10, 2]$
127	5	[6,6,8]	$[288, 10, 6]$
128	5	[8,8,8]	$[96, 10, 4]$
129	5	[16,16,8]	$[48, 10, 2]$
130	5	[6,6,9]	$[216, 10, 5]$
131	5	[12,12,9]	$[54, 10, 3]$
132	5	[6,6,10]	$[180, 10, 5]$
133	5	[10,10,10]	$[60, 10, 3]$
134	5	[6,6,12]	$[144, 10, 4]$
135	5	[8,8,12]	$[72, 10, 3]$
136	5	[24,24,12]	$[36, 10, 2]$
137	5	[6,6,14]	$[126, 10, 4]$
138	5	[14,14,14]	$[42, 10, 2]$
139	5	[12,12,15]	$[45, 10, 2]$
140	5	[6,6,18]	$[108, 10, 3]$
141	5	[8,8,20]	$[60, 10, 2]$
142	5	[40,40,20]	$[30, 10, 1]$

Códigos de Superfície Provenientes de Tesselações $[2p, 2q, 4]$ do g-toro, $g \geq 2$: O código quântico de superfície obtido a partir da tesselação semirregular $[2p, 2q, 4]$ situada sobre o g-toro, $g \geq 2$, derivada da tesselação regular $\{p, q\}$, é composto por $n = \dfrac{12pq(g-1)}{pq-2p-2q}$ qubits físicos, $k = 2g$ qubits lógicos e um limitante inferior para a distância deste é obtido pelo menor inteiro, não menor do que o mínimo do conjunto $\left\{\dfrac{d_{\mathbb{M}}}{L}, \dfrac{d_{\mathbb{M}}}{l/2}, \dfrac{d_{\mathbb{M}}}{a}, \dfrac{d_{\mathbb{M}}}{r}\right\}$, onde L é o comprimento de aresta da tesselação $[2p, 2q, 4]$, l, a e r são, respectivamente, o comprimento de aresta, de um apótema e do raio de um polígono da tesselação regular $\{p, q\}$.

Seguem abaixo algumas tabelas com os parâmetros de alguns dos códigos assim obtidos.

#	g	Tesselação	$[n, k, d]$
1	2	[6,14,4]	$[252, 4, 5]$
2	2	[6,16,4]	$[144, 4, 4]$
3	2	[6,18,4]	$[108, 4, 3]$
4	2	[6,20,4]	$[90, 4, 3]$
5	2	[6,24,4]	$[72, 4, 3]$
6	2	[8,10,4]	$[120, 4, 4]$
7	2	[8,12,4]	$[72, 4, 3]$
8	2	[8,16,4]	$[48, 4, 2]$
9	2	[8,24,4]	$[36, 4, 2]$
10	2	[10,8,4]	$[120, 4, 4]$
11	2	[10,10,4]	$[60, 4, 3]$
12	2	[10,20,4]	$[30, 4, 2]$
13	2	[12,8,4]	$[72, 4, 3]$
14	2	[12,12,4]	$[36, 4, 2]$
15	2	[14,6,4]	$[252, 4, 5]$
16	2	[16,6,4]	$[144, 4, 4]$
17	2	[16,8,4]	$[48, 4, 2]$
18	2	[16,16,4]	$[24, 4, 2]$
19	2	[18,6,4]	$[108, 4, 3]$
20	2	[20,6,4]	$[90, 4, 3]$
21	2	[20,10,4]	$[30, 4, 2]$
22	2	[24,6,4]	$[72, 4, 3]$
23	2	[24,8,4]	$[36, 4, 2]$

#	g	Tesselação	$[n, k, d]$
24	3	[6,14,4]	$[504, 6, 7]$
25	3	[6,16,4]	$[288, 6, 5]$
26	3	[6,18,4]	$[216, 6, 4]$
27	3	[6,20,4]	$[180, 6, 4]$

#	g	Tesselação	$[n, k, d]$
28	3	[6,24,4]	$[144, 6, 3]$
29	3	[6,28,4]	$[126, 6, 3]$
30	3	[8,10,4]	$[240, 6, 5]$
31	3	[8,12,4]	$[144, 6, 4]$
32	3	[8,16,4]	$[96, 6, 3]$
33	3	[8,24,4]	$[72, 6, 2]$
34	3	[10,8,4]	$[240, 6, 5]$
35	3	[10,10,4]	$[120, 6, 4]$
36	3	[10,12,4]	$[90, 6, 3]$
37	3	[10,20,4]	$[60, 6, 2]$
38	3	[12,8,4]	$[144, 6, 4]$
39	3	[12,10,4]	$[90, 6, 3]$
40	3	[12,12,4]	$[72, 6, 3]$
41	3	[12,18,4]	$[54, 6, 2]$
42	3	[14,6,4]	$[504, 6, 7]$
43	3	[14,28,4]	$[42, 6, 2]$
44	3	[16,6,4]	$[288, 6, 5]$
45	3	[16,8,4]	$[96, 6, 3]$
46	3	[16,16,4]	$[48, 6, 2]$
47	3	[18,6,4]	$[216, 6, 4]$
48	3	[18,12,4]	$[54, 6, 2]$
49	3	[20,6,4]	$[180, 6, 4]$
50	3	[20,10,4]	$[60, 6, 2]$
51	3	[24,6,4]	$[144, 6, 3]$
52	3	[24,8,4]	$[72, 6, 2]$
53	3	[24,24,4]	$[36, 6, 2]$
54	3	[28,6,4]	$[126, 6, 3]$
55	3	[28,14,4]	$[42, 6, 2]$

#	g	Tesselação	$[n, k, d]$
56	4	[6,14,4]	$[756, 8, 8]$
57	4	[6,16,4]	$[432, 8, 6]$
58	4	[6,18,4]	$[324, 8, 5]$
59	4	[6,20,4]	$[270, 8, 4]$
60	4	[6,24,4]	$[216, 8, 4]$
61	4	[6,30,4]	$[180, 8, 3]$
62	4	[8,10,4]	$[360, 8, 6]$
63	4	[8,12,4]	$[216, 8, 5]$
64	4	[8,14,4]	$[168, 8, 4]$
65	4	[8,16,4]	$[144, 8, 4]$
66	4	[8,20,4]	$[120, 8, 3]$
67	4	[8,24,4]	$[108, 8, 3]$
68	4	[10,8,4]	$[360, 8, 6]$
69	4	[10,10,4]	$[180, 8, 4]$
70	4	[10,20,4]	$[90, 8, 3]$
71	4	[12,8,4]	$[216, 8, 5]$
72	4	[12,12,4]	$[108, 8, 3]$
73	4	[12,24,4]	$[72, 8, 2]$
74	4	[14,6,4]	$[756, 8, 8]$
75	4	[14,8,4]	$[168, 8, 4]$
76	4	[14,14,4]	$[84, 8, 3]$
77	4	[16,6,4]	$[432, 8, 6]$
78	4	[16,8,4]	$[144, 8, 4]$
79	4	[16,16,4]	$[72, 8, 2]$
80	4	[18,6,4]	$[324, 8, 5]$
81	4	[20,6,4]	$[270, 8, 4]$
82	4	[20,8,4]	$[120, 8, 3]$
83	4	[20,10,4]	$[90, 8, 3]$
84	4	[20,20,4]	$[60, 8, 2]$
85	4	[24,6,4]	$[216, 8, 4]$
86	4	[24,8,4]	$[108, 8, 3]$
87	4	[24,12,4]	$[72, 8, 2]$
88	4	[30,6,4]	$[180, 8, 3]$

#	g	Tesselação	$[n, k, d]$
89	5	[6,14,4]	$[1008, 10, 9]$
90	5	[6,16,4]	$[576, 10, 6]$
91	5	[6,18,4]	$[432, 10, 5]$
92	5	[6,20,4]	$[360, 10, 5]$
93	5	[6,24,4]	$[288, 10, 4]$
94	5	[6,28,4]	$[252, 10, 4]$
95	5	[8,10,4]	$[480, 10, 7]$
96	5	[8,12,4]	$[288, 10, 5]$
97	5	[8,16,4]	$[192, 10, 4]$
98	5	[8,24,4]	$[144, 10, 3]$
99	5	[10,8,4]	$[480, 10, 7]$
100	5	[10,10,4]	$[240, 10, 5]$
101	5	[10,12,4]	$[180, 10, 4]$
102	5	[10,20,4]	$[120, 10, 3]$
103	5	[12,8,4]	$[288, 10, 5]$
104	5	[12,10,4]	$[180, 10, 4]$
105	5	[12,12,4]	$[144, 10, 3]$
106	5	[12,14,4]	$[126, 10, 3]$
107	5	[12,18,4]	$[108, 10, 3]$
108	5	[12,30,4]	$[90, 10, 2]$
109	5	[14,6,4]	$[1008, 10, 9]$
110	5	[14,12,4]	$[126, 10, 3]$
111	5	[14,28,4]	$[84, 10, 2]$
112	5	[16,6,4]	$[576, 10, 6]$
113	5	[16,8,4]	$[192, 10, 4]$
114	5	[16,16,4]	$[96, 10, 3]$
115	5	[18,6,4]	$[432, 10, 5]$
116	5	[18,12,4]	$[108, 10, 3]$
117	5	[20,6,4]	$[360, 10, 5]$
118	5	[20,10,4]	$[120, 10, 3]$
119	5	[24,6,4]	$[288, 10, 4]$
120	5	[24,8,4]	$[144, 10, 3]$
121	5	[24,24,4]	$[72, 10, 2]$
122	5	[28,6,4]	$[252, 10, 4]$
123	5	[28,14,4]	$[84, 10, 2]$
124	5	[30,12,4]	$[90, 10, 2]$

4.2 Códigos de Superfície Obtidos por Tesselações Semirregulares $[2p_1, \dots, 2p_t]$ do g-toro ($g \geq 2$)

Com base no teorema 1.6.1, mais especificamente, no corolário 1.6.3, dados inteiros positivos $g \geq 2$, $p_1, \cdots, p_t$, R, E, $V_1, \cdots, V_t$, tais que $R = \frac{^{4(g-1)}\prod_j p_j}{^{(t-2)}\prod_j p_j - \sum_i \prod_{j \neq i} p_j}$, $E = \frac{tR}{2}$ e $V_i = \frac{R}{2p_i}$, existe uma tesselação semirregular $[2p_1, \cdots, 2p_t]$ do g-toro $\mathbb{M}$, a qual conta com E arestas, R vértices, $F = \sum_i V_i$ faces, das quais $\frac{R}{2p_i}$ são $2p_i$-gons.

Estas tesselações fornecem, assim como antes, códigos quânticos de superfície. A construção deste é inteiramente análoga à feita na seção 3.8.2 do capítulo 3.

Mais especificamente, sejam $\mathcal{V}$, $\mathcal{E}$ e $\mathcal{F}$ os conjuntos de vértices, arestas e faces da tesselação e considere $\mathcal{H} = \bigotimes_{e \in \mathcal{E}} \mathbb{C}^2$ como sendo o espaço do sistema ao qual os qubits pertencem. Defina, para cada $f \in \mathcal{F}$, o operador $\mathfrak{X}_f = \bigotimes_{e \in \mathcal{E}} \mathfrak{X}^{\delta(e \in \mathcal{E}_f)}$ e, similarmente, para cada $v \in \mathcal{V}$, o operador $\mathfrak{Z}_v = \bigotimes_{e \in \mathcal{E}} \mathfrak{Z}^{\delta(e \in \mathcal{E}_v)}$. Obviamente estes operadores atuam sobre o espaço $\mathcal{H}$. Observa-se que, para cada $v \in \mathcal{V}$ e para cada $f \in \mathcal{F}$, os conjuntos $\mathcal{E}_f$ e $\mathcal{E}_v$ possuem zero ou dois elementos em comum e, portanto, $\mathfrak{X}_f$ e $\mathfrak{Z}_v$ comutam. Desta forma, $\mathcal{S}_{est} = \langle \mathfrak{X}_f, \mathfrak{Z}_v \rangle$ é um grupo abeliano.

Denote por $\mathcal{C}$ o subespaço vetorial de $\mathcal{H}$ obtido pela intersecção dos auto-espaços associados ao autovetor $+1$ de cada um destes operadores:

$$\mathcal{C} = \{|\varphi\rangle \in \mathcal{H} / \mathfrak{X}_f |\varphi\rangle = \mathfrak{Z}_v |\varphi\rangle = |\varphi\rangle, f \in \mathcal{F}, v \in \mathcal{V}\}$$

Observação 4.2.1. Se $\mathcal{V}$, $\mathcal{E}$ e $\mathcal{F}$ são, respectivamente, os conjuntos de vértices, arestas e faces da tesselação, tem-se $\#\mathcal{V} = R$, $\#\mathcal{E} = E$ e $\#\mathcal{F} = F$.

Proposição 4.2.2. $Id \notin \mathcal{S}_{est}$.

Demonstração: Suponha, por absurdo, que $-Id \in \mathcal{S}_{est}$. Para tal, devem existir subconjuntos $\mathcal{F}_0 \subset \mathcal{F}$ e $\mathcal{V}_0 \subset \mathcal{V}$, tais que $\left(\prod_{f \in \mathcal{F}_0} \mathfrak{X}_f\right)\left(\prod_{v \in \mathcal{V}_0} \mathfrak{Z}_v\right) = -Id$, de onde segue que $\prod_{f \in \mathcal{F}_0} \mathfrak{X}_f = -\prod_{v \in \mathcal{V}_0} \mathfrak{Z}_v$. Note que $\mathcal{F}_0 \neq \mathcal{F}$ ou $\mathcal{V}_0 \neq \mathcal{V}$. Se $\mathcal{F}_0 \neq \mathcal{F}$, existe $f_0 \in \mathcal{F}_0$, tal que $\mathfrak{Z}_{f_0}\left(\prod_{f \in \mathcal{F}_0} \mathfrak{X}_f\right) =$

$-\left(\prod_{f\in\mathcal{F}_0} \mathfrak{X}_f\right)\mathfrak{Z}_{f_0}$. Assim,

$$\begin{aligned}\prod_{f\in\mathcal{F}_0}\mathfrak{X}_f &= \mathfrak{Z}_{f_0}^2\left(\prod_{f\in\mathcal{F}_0}\mathfrak{X}_f\right) &&= -\mathfrak{Z}_{f_0}\left(\prod_{f\in\mathcal{F}_0}\mathfrak{X}_f\right)\mathfrak{Z}_{f_0}\\ &= -\mathfrak{Z}_{f_0}\left(-\prod_{v\in\mathcal{V}}\mathfrak{Z}_v\right)\mathfrak{Z}_{f_0} &&= \mathfrak{Z}_{f_0}^2\left(\prod_{v\in\mathcal{V}}\mathfrak{Z}_v\right)\\ &= \prod_{v\in\mathcal{V}}\mathfrak{Z}_v &&= -\prod_{f\in\mathcal{F}_0}\mathfrak{X}_f.\end{aligned}$$

de onde segue que $\prod_{f\in\mathcal{F}_0}\mathfrak{X}_f = 0 \notin \mathcal{S}_{est}$. O caso em que $\mathcal{V}_0 \neq \mathcal{V}$ é tratado de forma análoga.□

Conforme antes observado, $\prod_{f\in\mathcal{F}}\mathfrak{X}_f = \prod_{v\in\mathcal{V}}\mathfrak{Z}_v = Id$. Com isto, para cada $f_0 \in \mathcal{F}$, tem-se

$$\begin{aligned}\prod_{f\in\mathcal{F}, f\neq f_0}\mathfrak{X}_f &= \prod_{f\in\mathcal{F}, f\neq f_0}\left(\bigotimes_{e\in\mathcal{E}}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\ &= \bigotimes_{e\in\mathcal{E}}\left(\prod_{f\in\mathcal{F}, f\neq f_0}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\ &= \bigotimes_{e\in\mathcal{E}}\left(\mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})}\prod_{f\in\mathcal{V}}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\ &= \left(\bigotimes_{e\in\mathcal{E}}\mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})}\right)\left(\bigotimes_{e\in\mathcal{E}}\prod_{f\in\mathcal{F}}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\ &= \left(\bigotimes_{e\in\mathcal{E}}\mathfrak{X}^{\delta(e\in\mathcal{E}_{f_0})}\right)\left(\prod_{f\in\mathcal{V}}\bigotimes_{e\in\mathcal{E}}\mathfrak{X}^{\delta(e\in\mathcal{E}_f)}\right)\\ &= \mathfrak{X}_{f_0}\prod_{f\in\mathcal{F}}\mathfrak{X}_f\\ &= \mathfrak{X}_{f_0}Id\\ &= \mathfrak{X}_{f_0}.\end{aligned}$$

Analogamente, para cada $v_0 \in \mathcal{V}$ fixada, tem-se $\prod_{v\in\mathcal{V}, v\neq v_0}\mathfrak{Z}_v = \mathfrak{Z}_{v_0}$.

Assim, $\mathcal{S}_{est}$ possui $\#\mathcal{F}-1+\#\mathcal{V}-1$ geradores independentes. Portanto, o código $\mathcal{C}$ codifica $k = n - (\#\mathcal{F} + \#\mathcal{V} - 2)$ qubits. Assim,

$$\begin{aligned} k &= n - (\#\mathcal{F} + \#\mathcal{V} - 2) \\ &= \#\mathcal{E} - \#\mathcal{F} - \#\mathcal{V} + 2 \\ &= -(\#\mathcal{F} - \#\mathcal{E} + \#\mathcal{V}) + 2 \\ &= -\chi(\mathbb{M}) + 2 \\ &= -2(1-g) + 2 \\ &= 2g. \end{aligned}$$

O número de qubits físicos é exatamente $\#\mathcal{E}$, enquanto que o número de qubits lógicos é $2g$. Se $\mathcal{S}_{est}$ é o grupo estabilizador deste código, um operador pertencente a $\mathcal{C}(\mathcal{S}_{est}) - \mathcal{S}_{est}$ está biunivocamente determinado por um segmento de grafo contido na tesselação que tem homologia não trivial. Em síntese, sabemos que este deve ser um ciclo de homologia não trivial. Tal qual feito em [21], podemos estimar um limitante inferior para esta cadeia de erros dividindo o diâmetro do polígono da tesselação $\{4g, 4g\}$ pelo comprimento de arestas da tesselação, bem como de sua dual, e arredondar para maior, o menor dentre estes valores. As medidas de aresta empregadas neste cálculo são obtidas com o uso da Proposição 1.6.4.

Com este processo, obtemos os códigos cujos parâmetros estão listados nas tabelas abaixo.

Esta construção fornece como caso particular os códigos de superfície de [21].

Tabela 4.1: Tabela de Parâmetros dos Códigos de Superfície Provenientes de Tesselações Semirregulares sobre o 2-Toro.

#	g	Tesselação	$[n,k,d]$
1	2	[10,10,10]	[15,4,2]
2	2	[8,8,8]	[24,4,3]
3	2	[6,12,12]	[18,4,2]
4	2	[4,6,18]	[108,4,3]
5	2	[4,8,4,8]	[16,4,3]
6	2	[4,4,6,6]	[24,4,3]
7	2	[4,4,8,8]	[16,4,2]
8	2	[4,4,4,8]	[32,4,3]
9	2	[4,4,4,4,4]	[20,4,3]
10	2	[4,4,4,4,4,4]	[12,4,2]

Tabela 4.2: Tabela de Parâmetros dos Códigos de Superfície Provenientes de Tesselações Semirregulares sobre o 3-Toro.

#	g	Tesselação	$[n, k, d]$
11	3	[8,8,12]	[36,6,3]
12	3	[4,12,4,12]	[24,6,3]
13	3	[8,8,8,8]	[16,6,2]
14	3	[4,8,4,8]	[32,6,3]
15	3	[4,4,12,12]	[24,6,2]
16	3	[4,6,4,6]	[48,6,4]
17	3	[4,4,8,4,8]	[20,6,3]
18	3	[6,6,6,6,6]	[15,6,2]
19	3	[4,4,4,4,6]	[30,6,3]
20	3	[4,4,4,8,8]	[20,6,2]

Tabela 4.3: Tabela de Parâmetros dos Códigos de Superfície Provenientes de Tesselações Semirregulares sobre o 4-Toro.

#	g	Tesselação	$[n, k, d]$
21	4	[18,18,18]	[27,8,2]
22	4	[10,10,10,10]	[20,8,2]
23	4	[4,8,8,8]	[32,8,3]
24	4	[4,12,12,12]	[24,8,2]
25	4	[4,10,4,10]	[40,8,3]
26	4	[4,4,6,4,12]	[30,8,3]
27	4	[6,6,6,6,6,6]	[18,8,3]
28	4	[4,4,4,8,4,8]	[24,8,3]
29	4	[4,4,4,4,4,4]	[36,8,3]
30	4	[4,4,4,4,8,8]	[24,8,2]

Tabela 4.4: Tabela de Parâmetros dos Códigos de Superfície Provenientes de Tesselações Semirregulares sobre o 5-Toro.

#	g	Tesselação	$[n, k, d]$
31	5	[6,14,14]	[63, 10, 2]
32	5	[12,12,12,12]	[24, 10, 2]
33	5	[4,6,6,12]	[48, 10, 3]
34	5	[4,8,4,8]	[64, 10, 4]
35	5	[4,8,16,16]	[32, 10, 2]
36	5	[6,6,6,6,6]	[30, 10, 3]
37	5	[4,4,8,4,8]	[40, 10, 3]
38	5	[4,4,6,12,12]	[30, 10, 2]
39	5	[4,4,4,4,4,12]	[36, 10, 3]
40	5	[4,4,8,8,8,8]	[24, 10, 2]

4.2.1 Elementos Gráficos

Seguem abaixo gráficos comparativos entre os códigos de superfície gerados a partir de tesselações regulares e semirregulares sobre superfícies de gênus de 2 a 5.

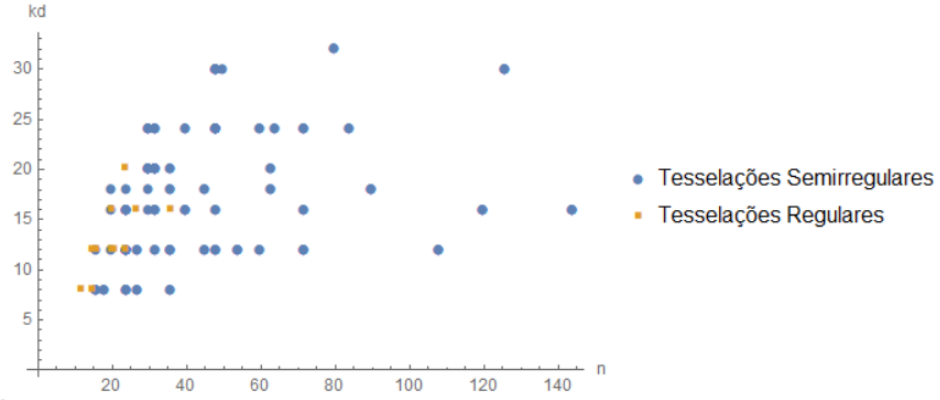


Figura 4.1: Distribuição dos parâmetros kd, no eixo vertical, em relação à quantidade de qubits físicos n, no eixo horizontal.

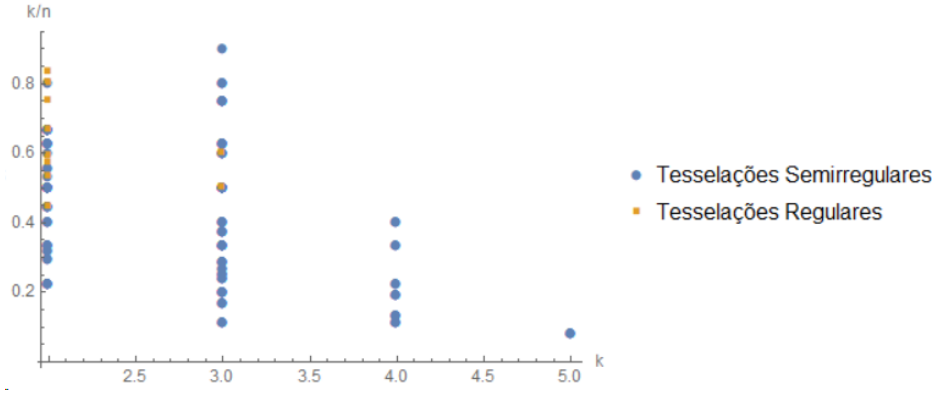


Figura 4.2: Distribuição dos parâmetros k/n, no eixo vertical, em relação à quantidade de qubits lógicos k, no eixo horizontal.

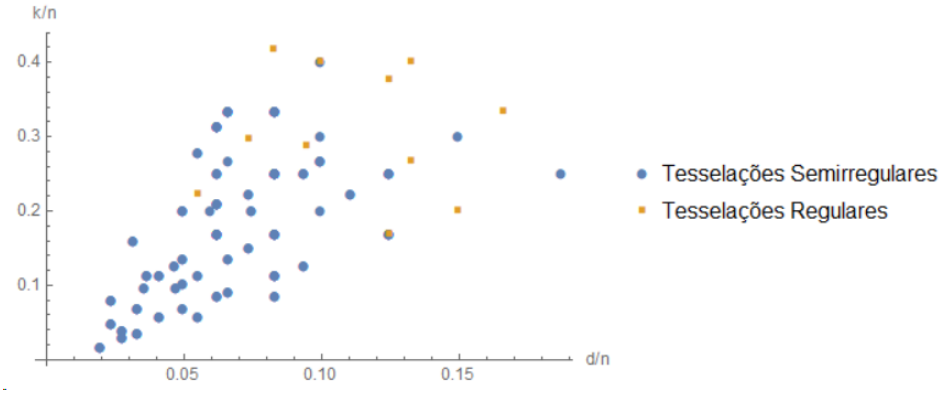


Figura 4.3: Distribuição dos parâmetros k/n, no eixo vertical, em relação aos parâmetros d/n, no eixo horizontal.

Capítulo 5

Novos Códigos Quânticos Coloridos

Neste capítulo estudamos os códigos coloridos obtidos das tesselações semirregulares trivalentes e 3-coloríveis do g-toro, $g \geq 2$. Em particular, a partir das tesselações derivadas estudadas na seção 1.5.3, constrói-se os códigos coloridos da seção 5.1.

5.1 Códigos Coloridos Provenientes das Tesselações Semirregulares $[2p, 2p, q]$ e $[2p, 2q, 4]$ do g-toro

Como introdução aos resultados da presente tese, no que tange aos códigos quânticos coloridos estabelecidos através de tesselações semirregulares do g-toro, $g \geq 2$, apresentamos abaixo duas famílias de códigos de superfície provenientes das tesselações derivadas. A seção subsequente a isto, cito 5.2, contém o estudo dos códigos quânticos coloridos obtidos de tesselações semirregulares construídas intrinsecamente sobre o g-toro, $g \geq 2$, sem a dependência de tesselações regulares preexistentes.

Observação 5.1.1. Conforme a observação 1.5.17, a tesselação $[2p, 2p, q]$, derivada da tesselação regular $\{p, q\}$, possui $N_f = \frac{4(p+q)(g-1)}{pq-2p-2q}$ faces, $N_e = \frac{6pq(g-1)}{pq-2p-2q}$ arestas e $N_v = \frac{4pq(g-1)}{pq-2p-2q}$ vértices, enquanto que a tesselação $[2p, 2q, 4]$, derivada da tesselação regular $\{p, q\}$, possui $N_f = \frac{2(pq+2p+2q)(g-1)}{pq-2p-2q}$ faces, $N_e = \frac{12pq(g-1)}{pq-2p-2q}$ arestas e $N_v = \frac{8pq(g-1)}{pq-2p-2q}$ vértices.

Códigos Coloridos Provenientes de Tesselações $[2p, 2p, q]$ do g-toro, $g \geq 2$: Similarmente ao que se encontra na seção 3.8.3, dada a tesselação $[2p, 2p, q]$ do g-toro, $g \geq 2$, admitindo que esta seja 3-colorível, pode-se construir um operador face, para cada uma das

faces da tesselação $[2p, 2p, q]$, obtendo-se assim, um código quântico colorido, cujo comprimento é de $n = \dfrac{4pq(g-1)}{pq-2p-2q}$ qubits físicos, nos quais se codificam $k = 4g$ qubits lógicos.

Códigos Coloridos Provenientes de Tesselações $[2p, 2q, 4]$ do g-toro, $g \geq 2$: Similarmente ao que se encontra na seção 3.8.3 e no parágrafo anterior, dada a tesselação $[2p, 2q, 4]$ do g-toro, $g \geq 2$, admitindo que esta seja 3-colorível, pode-se construir um operador face, para cada uma das faces da tesselação $[2p, 2q, 4]$, obtendo-se assim, um código quântico colorido, cujo comprimento é de $n = \dfrac{8pq(g-1)}{pq-2p-2q}$ qubits físicos, nos quais se codificam $k = 4g$ qubits lógicos.

Salientamos que o caso em que $p = q$ é contemplado pelo caso abordado acima e que, caso $p \neq q$, a tesselação é 3-colorível, pois é constituída por faces de 3 polígonos dois a dois distintos.

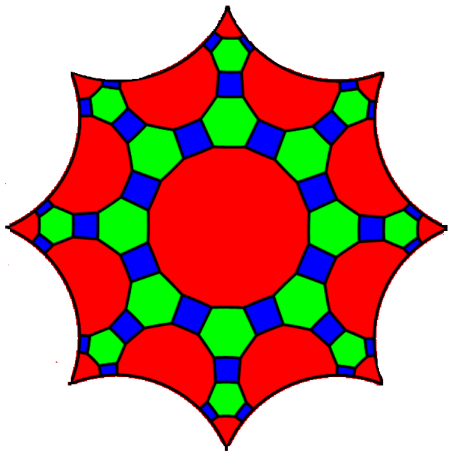


Figura 5.1: Tesselação semirregular $[16, 8, 4]$ sobre um domínio fundamental da tesselação regular $\{8, 8\}$, o qual fornece o 2-toro mediante quociente de grupo.

Exemplo 5.1.2. Abaixo encontra-se a figura 5.2, a qual traz uma representação da tesselação $[16, 8, 4]$ sobre o 2-toro. Encontram-se enumerados os 96 vértices.

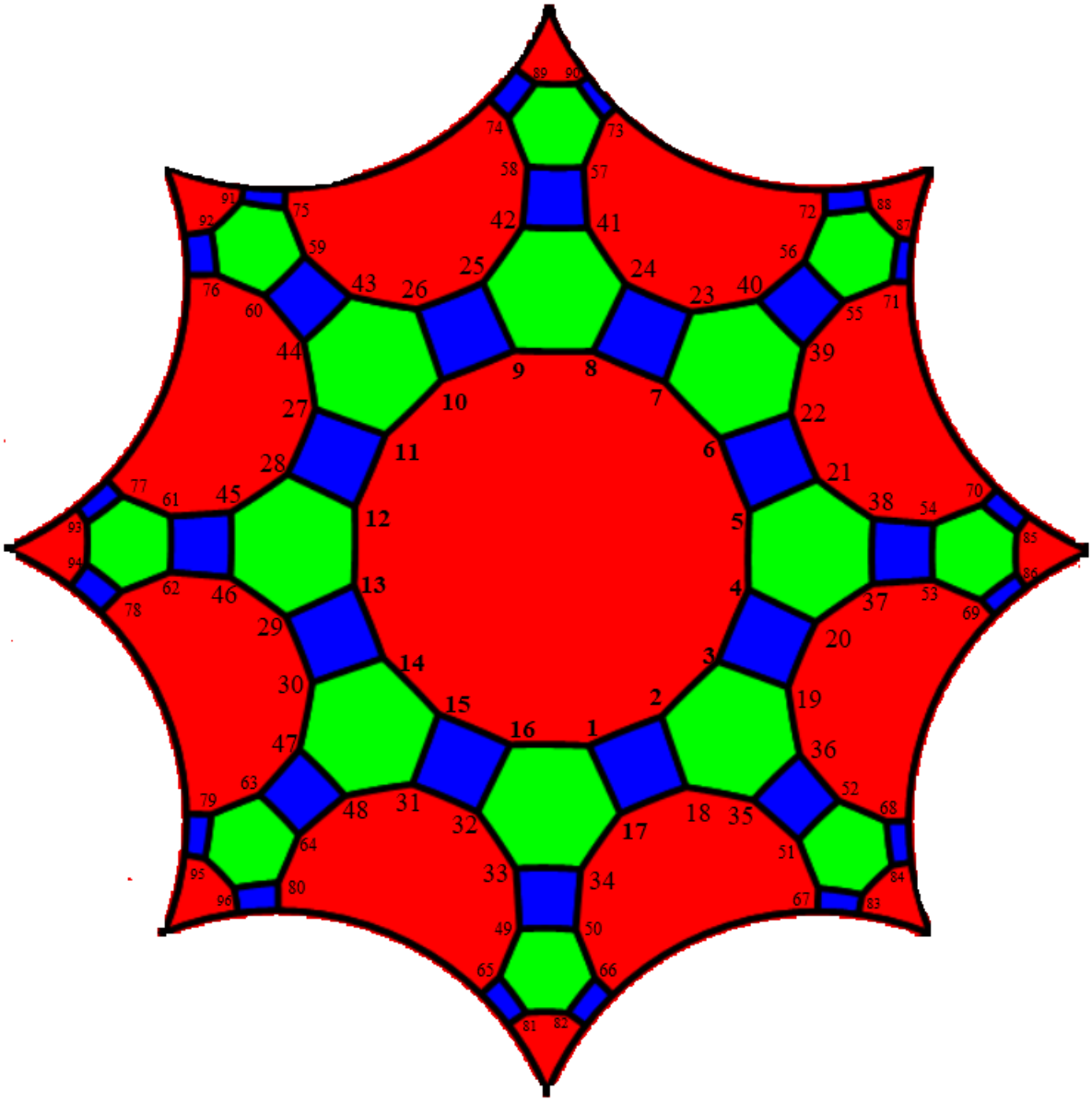


Figura 5.2: Tesselação Semirregular $[16, 8, 4]$ sobre um domínio fundamental da tesselação regular $\{8, 8\}$, o qual fornece o 2-toro mediante quociente de grupo.

Os operadores associados às faces são dados na tabela abaixo:

Tabela 5.1: Tabela contendo os operadores face que geram o grupo estabilizador do sódigo colorido proveniente da tesselação semirregular $[16, 8, 4]$ sobre o 2-toro.

$\mathfrak{X}_{(fr_1)} = \mathfrak{X}_1\mathfrak{X}_2\mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_8\mathfrak{X}_9\mathfrak{X}_{10}\mathfrak{X}_{11}\mathfrak{X}_{12}\mathfrak{X}_{13}\mathfrak{X}_{14}\mathfrak{X}_{15}\mathfrak{X}_{16}$	$\mathfrak{Z}_{(fr_1)} = \mathfrak{Z}_1\mathfrak{Z}_2\mathfrak{Z}_3\mathfrak{Z}_4\mathfrak{Z}_5\mathfrak{Z}_6\mathfrak{Z}_7\mathfrak{Z}_8\mathfrak{Z}_9\mathfrak{Z}_{10}\mathfrak{Z}_{11}\mathfrak{Z}_{12}\mathfrak{Z}_{13}\mathfrak{Z}_{14}\mathfrak{Z}_{15}\mathfrak{Z}_{16}$
$\mathfrak{X}_{(fr_2)} = \mathfrak{X}_{81}\mathfrak{X}_{82}\mathfrak{X}_{83}\mathfrak{X}_{84}\mathfrak{X}_{85}\mathfrak{X}_{86}\mathfrak{X}_{87}\mathfrak{X}_{88}\mathfrak{X}_{89}\mathfrak{X}_{90}\mathfrak{X}_{91}\mathfrak{X}_{92}\mathfrak{X}_{93}\mathfrak{X}_{94}\mathfrak{X}_{95}\mathfrak{X}_{96}$	$\mathfrak{Z}_{(fr_2)} = \mathfrak{Z}_{81}\mathfrak{Z}_{82}\mathfrak{Z}_{83}\mathfrak{Z}_{84}\mathfrak{Z}_{85}\mathfrak{Z}_{86}\mathfrak{Z}_{87}\mathfrak{Z}_{88}\mathfrak{Z}_{89}\mathfrak{Z}_{90}\mathfrak{Z}_{91}\mathfrak{Z}_{92}\mathfrak{Z}_{93}\mathfrak{Z}_{94}\mathfrak{Z}_{95}\mathfrak{Z}_{96}$
$\mathfrak{X}_{(fr_3)} = \mathfrak{X}_{68}\mathfrak{X}_{52}\mathfrak{X}_{36}\mathfrak{X}_{19}\mathfrak{X}_{20}\mathfrak{X}_{37}\mathfrak{X}_{53}\mathfrak{X}_{69}\mathfrak{X}_{76}\mathfrak{X}_{60}\mathfrak{X}_{44}\mathfrak{X}_{27}\mathfrak{X}_{28}\mathfrak{X}_{45}\mathfrak{X}_{61}\mathfrak{X}_{77}$	$\mathfrak{Z}_{(fr_3)} = \mathfrak{Z}_{68}\mathfrak{Z}_{52}\mathfrak{Z}_{36}\mathfrak{Z}_{19}\mathfrak{Z}_{20}\mathfrak{Z}_{37}\mathfrak{Z}_{53}\mathfrak{Z}_{69}\mathfrak{Z}_{76}\mathfrak{Z}_{60}\mathfrak{Z}_{44}\mathfrak{Z}_{27}\mathfrak{Z}_{28}\mathfrak{Z}_{45}\mathfrak{Z}_{61}\mathfrak{Z}_{77}$
$\mathfrak{X}_{(fr_4)} = \mathfrak{X}_{66}\mathfrak{X}_{50}\mathfrak{X}_{34}\mathfrak{X}_{17}\mathfrak{X}_{18}\mathfrak{X}_{35}\mathfrak{X}_{51}\mathfrak{X}_{67}\mathfrak{X}_{74}\mathfrak{X}_{58}\mathfrak{X}_{42}\mathfrak{X}_{25}\mathfrak{X}_{26}\mathfrak{X}_{43}\mathfrak{X}_{59}\mathfrak{X}_{75}$	$\mathfrak{Z}_{(fr_4)} = \mathfrak{Z}_{66}\mathfrak{Z}_{50}\mathfrak{Z}_{34}\mathfrak{Z}_{17}\mathfrak{Z}_{18}\mathfrak{Z}_{35}\mathfrak{Z}_{51}\mathfrak{Z}_{67}\mathfrak{Z}_{74}\mathfrak{Z}_{58}\mathfrak{Z}_{42}\mathfrak{Z}_{25}\mathfrak{Z}_{26}\mathfrak{Z}_{43}\mathfrak{Z}_{59}\mathfrak{Z}_{75}$
$\mathfrak{X}_{(fr_5)} = \mathfrak{X}_{80}\mathfrak{X}_{64}\mathfrak{X}_{48}\mathfrak{X}_{31}\mathfrak{X}_{32}\mathfrak{X}_{33}\mathfrak{X}_{49}\mathfrak{X}_{65}\mathfrak{X}_{72}\mathfrak{X}_{56}\mathfrak{X}_{40}\mathfrak{X}_{23}\mathfrak{X}_{24}\mathfrak{X}_{41}\mathfrak{X}_{57}\mathfrak{X}_{73}$	$\mathfrak{Z}_{(fr_5)} = \mathfrak{Z}_{80}\mathfrak{Z}_{64}\mathfrak{Z}_{48}\mathfrak{Z}_{31}\mathfrak{Z}_{32}\mathfrak{Z}_{33}\mathfrak{Z}_{49}\mathfrak{Z}_{65}\mathfrak{Z}_{72}\mathfrak{Z}_{56}\mathfrak{Z}_{40}\mathfrak{Z}_{23}\mathfrak{Z}_{24}\mathfrak{Z}_{41}\mathfrak{Z}_{57}\mathfrak{Z}_{73}$
$\mathfrak{X}_{(fr_6)} = \mathfrak{X}_{78}\mathfrak{X}_{62}\mathfrak{X}_{46}\mathfrak{X}_{29}\mathfrak{X}_{30}\mathfrak{X}_{47}\mathfrak{X}_{63}\mathfrak{X}_{79}\mathfrak{X}_{71}\mathfrak{X}_{55}\mathfrak{X}_{39}\mathfrak{X}_{22}\mathfrak{X}_{21}\mathfrak{X}_{38}\mathfrak{X}_{54}\mathfrak{X}_{70}$	$\mathfrak{Z}_{(fr_6)} = \mathfrak{Z}_{78}\mathfrak{Z}_{62}\mathfrak{Z}_{46}\mathfrak{Z}_{29}\mathfrak{Z}_{30}\mathfrak{Z}_{47}\mathfrak{Z}_{63}\mathfrak{Z}_{79}\mathfrak{Z}_{71}\mathfrak{Z}_{55}\mathfrak{Z}_{39}\mathfrak{Z}_{22}\mathfrak{Z}_{21}\mathfrak{Z}_{38}\mathfrak{Z}_{54}\mathfrak{Z}_{70}$
$\mathfrak{X}_{(fg_1)} = \mathfrak{X}_1\mathfrak{X}_{16}\mathfrak{X}_{17}\mathfrak{X}_{32}\mathfrak{X}_{33}\mathfrak{X}_{34}$	$\mathfrak{Z}_{(fg_1)} = \mathfrak{Z}_1\mathfrak{Z}_{16}\mathfrak{Z}_{17}\mathfrak{Z}_{32}\mathfrak{Z}_{33}\mathfrak{Z}_{34}$
$\mathfrak{X}_{(fg_2)} = \mathfrak{X}_2\mathfrak{X}_3\mathfrak{X}_{18}\mathfrak{X}_{19}\mathfrak{X}_{35}\mathfrak{X}_{36}$	$\mathfrak{Z}_{(fg_2)} = \mathfrak{Z}_2\mathfrak{Z}_3\mathfrak{Z}_{18}\mathfrak{Z}_{19}\mathfrak{Z}_{35}\mathfrak{Z}_{36}$
$\mathfrak{X}_{(fg_3)} = \mathfrak{X}_4\mathfrak{X}_5\mathfrak{X}_{20}\mathfrak{X}_{21}\mathfrak{X}_{37}\mathfrak{X}_{38}$	$\mathfrak{Z}_{(fg_3)} = \mathfrak{Z}_4\mathfrak{Z}_5\mathfrak{Z}_{20}\mathfrak{Z}_{21}\mathfrak{Z}_{37}\mathfrak{Z}_{38}$
$\mathfrak{X}_{(fg_4)} = \mathfrak{X}_6\mathfrak{X}_7\mathfrak{X}_{22}\mathfrak{X}_{23}\mathfrak{X}_{39}\mathfrak{X}_{40}$	$\mathfrak{Z}_{(fg_4)} = \mathfrak{Z}_6\mathfrak{Z}_7\mathfrak{Z}_{22}\mathfrak{Z}_{23}\mathfrak{Z}_{39}\mathfrak{Z}_{40}$
$\mathfrak{X}_{(fg_5)} = \mathfrak{X}_8\mathfrak{X}_9\mathfrak{X}_{24}\mathfrak{X}_{25}\mathfrak{X}_{41}\mathfrak{X}_{42}$	$\mathfrak{Z}_{(fg_5)} = \mathfrak{Z}_8\mathfrak{Z}_9\mathfrak{Z}_{24}\mathfrak{Z}_{25}\mathfrak{Z}_{41}\mathfrak{Z}_{42}$
$\mathfrak{X}_{(fg_6)} = \mathfrak{X}_{10}\mathfrak{X}_{11}\mathfrak{X}_{26}\mathfrak{X}_{27}\mathfrak{X}_{43}\mathfrak{X}_{44}$	$\mathfrak{Z}_{(fg_6)} = \mathfrak{Z}_{10}\mathfrak{Z}_{11}\mathfrak{Z}_{26}\mathfrak{Z}_{27}\mathfrak{Z}_{43}\mathfrak{Z}_{44}$
$\mathfrak{X}_{(fg_7)} = \mathfrak{X}_{12}\mathfrak{X}_{13}\mathfrak{X}_{28}\mathfrak{X}_{29}\mathfrak{X}_{45}\mathfrak{X}_{46}$	$\mathfrak{Z}_{(fg_7)} = \mathfrak{Z}_{12}\mathfrak{Z}_{13}\mathfrak{Z}_{28}\mathfrak{Z}_{29}\mathfrak{Z}_{45}\mathfrak{Z}_{46}$
$\mathfrak{X}_{(fg_8)} = \mathfrak{X}_{14}\mathfrak{X}_{15}\mathfrak{X}_{30}\mathfrak{X}_{31}\mathfrak{X}_{47}\mathfrak{X}_{48}$	$\mathfrak{Z}_{(fg_8)} = \mathfrak{Z}_{14}\mathfrak{Z}_{15}\mathfrak{Z}_{30}\mathfrak{Z}_{31}\mathfrak{Z}_{47}\mathfrak{Z}_{48}$
$\mathfrak{X}_{(fg_9)} = \mathfrak{X}_{49}\mathfrak{X}_{50}\mathfrak{X}_{65}\mathfrak{X}_{66}\mathfrak{X}_{81}\mathfrak{X}_{82}$	$\mathfrak{Z}_{(fg_9)} = \mathfrak{Z}_{49}\mathfrak{Z}_{50}\mathfrak{Z}_{65}\mathfrak{Z}_{66}\mathfrak{Z}_{81}\mathfrak{Z}_{82}$
$\mathfrak{X}_{(fg_{10})} = \mathfrak{X}_{51}\mathfrak{X}_{52}\mathfrak{X}_{67}\mathfrak{X}_{68}\mathfrak{X}_{83}\mathfrak{X}_{84}$	$\mathfrak{Z}_{(fg_{10})} = \mathfrak{Z}_{51}\mathfrak{Z}_{52}\mathfrak{Z}_{67}\mathfrak{Z}_{68}\mathfrak{Z}_{83}\mathfrak{Z}_{84}$
$\mathfrak{X}_{(fg_{11})} = \mathfrak{X}_{53}\mathfrak{X}_{54}\mathfrak{X}_{69}\mathfrak{X}_{70}\mathfrak{X}_{85}\mathfrak{X}_{86}$	$\mathfrak{Z}_{(fg_{11})} = \mathfrak{Z}_{53}\mathfrak{Z}_{54}\mathfrak{Z}_{69}\mathfrak{Z}_{70}\mathfrak{Z}_{85}\mathfrak{Z}_{86}$
$\mathfrak{X}_{(fg_{12})} = \mathfrak{X}_{55}\mathfrak{X}_{56}\mathfrak{X}_{71}\mathfrak{X}_{72}\mathfrak{X}_{87}\mathfrak{X}_{88}$	$\mathfrak{Z}_{(fg_{12})} = \mathfrak{Z}_{55}\mathfrak{Z}_{56}\mathfrak{Z}_{71}\mathfrak{Z}_{72}\mathfrak{Z}_{87}\mathfrak{Z}_{88}$
$\mathfrak{X}_{(fg_{13})} = \mathfrak{X}_{57}\mathfrak{X}_{58}\mathfrak{X}_{73}\mathfrak{X}_{74}\mathfrak{X}_{89}\mathfrak{X}_{90}$	$\mathfrak{Z}_{(fg_{13})} = \mathfrak{Z}_{57}\mathfrak{Z}_{58}\mathfrak{Z}_{73}\mathfrak{Z}_{74}\mathfrak{Z}_{89}\mathfrak{Z}_{90}$
$\mathfrak{X}_{(fg_{14})} = \mathfrak{X}_{59}\mathfrak{X}_{60}\mathfrak{X}_{75}\mathfrak{X}_{76}\mathfrak{X}_{91}\mathfrak{X}_{92}$	$\mathfrak{Z}_{(fg_{14})} = \mathfrak{Z}_{59}\mathfrak{Z}_{60}\mathfrak{Z}_{75}\mathfrak{Z}_{76}\mathfrak{Z}_{91}\mathfrak{Z}_{92}$
$\mathfrak{X}_{(fg_{15})} = \mathfrak{X}_{61}\mathfrak{X}_{62}\mathfrak{X}_{77}\mathfrak{X}_{78}\mathfrak{X}_{93}\mathfrak{X}_{94}$	$\mathfrak{Z}_{(fg_{15})} = \mathfrak{Z}_{61}\mathfrak{Z}_{62}\mathfrak{Z}_{77}\mathfrak{Z}_{78}\mathfrak{Z}_{93}\mathfrak{Z}_{94}$
$\mathfrak{X}_{(fg_{16})} = \mathfrak{X}_{63}\mathfrak{X}_{64}\mathfrak{X}_{79}\mathfrak{X}_{80}\mathfrak{X}_{95}\mathfrak{X}_{96}$	$\mathfrak{Z}_{(fg_{16})} = \mathfrak{Z}_{63}\mathfrak{Z}_{64}\mathfrak{Z}_{79}\mathfrak{Z}_{80}\mathfrak{Z}_{95}\mathfrak{Z}_{96}$
$\mathfrak{X}_{(fb_1)} = \mathfrak{X}_{90}\mathfrak{X}_{73}\mathfrak{X}_{80}\mathfrak{X}_{96}$	$\mathfrak{Z}_{(fb_1)} = \mathfrak{Z}_{90}\mathfrak{Z}_{73}\mathfrak{Z}_{80}\mathfrak{Z}_{96}$
$\mathfrak{X}_{(fb_2)} = \mathfrak{X}_{72}\mathfrak{X}_{88}\mathfrak{X}_{65}\mathfrak{X}_{81}$	$\mathfrak{Z}_{(fb_2)} = \mathfrak{Z}_{72}\mathfrak{Z}_{88}\mathfrak{Z}_{65}\mathfrak{Z}_{81}$
$\mathfrak{X}_{(fb_3)} = \mathfrak{X}_{71}\mathfrak{X}_{87}\mathfrak{X}_{78}\mathfrak{X}_{94}$	$\mathfrak{Z}_{(fb_3)} = \mathfrak{Z}_{71}\mathfrak{Z}_{87}\mathfrak{Z}_{78}\mathfrak{Z}_{94}$
$\mathfrak{X}_{(fb_4)} = \mathfrak{X}_{70}\mathfrak{X}_{85}\mathfrak{X}_{95}\mathfrak{X}_{79}$	$\mathfrak{Z}_{(fb_4)} = \mathfrak{Z}_{70}\mathfrak{Z}_{85}\mathfrak{Z}_{95}\mathfrak{Z}_{79}$
$\mathfrak{X}_{(fb_5)} = \mathfrak{X}_{69}\mathfrak{X}_{86}\mathfrak{X}_{92}\mathfrak{X}_{76}$	$\mathfrak{Z}_{(fb_5)} = \mathfrak{Z}_{69}\mathfrak{Z}_{86}\mathfrak{Z}_{92}\mathfrak{Z}_{76}$
$\mathfrak{X}_{(fb_6)} = \mathfrak{X}_{68}\mathfrak{X}_{84}\mathfrak{X}_{93}\mathfrak{X}_{77}$	$\mathfrak{Z}_{(fb_6)} = \mathfrak{Z}_{68}\mathfrak{Z}_{84}\mathfrak{Z}_{93}\mathfrak{Z}_{77}$
$\mathfrak{X}_{(fb_7)} = \mathfrak{X}_{67}\mathfrak{X}_{83}\mathfrak{X}_{74}\mathfrak{X}_{89}$	$\mathfrak{Z}_{(fb_7)} = \mathfrak{Z}_{67}\mathfrak{Z}_{83}\mathfrak{Z}_{74}\mathfrak{Z}_{89}$
$\mathfrak{X}_{(fb_8)} = \mathfrak{X}_{66}\mathfrak{X}_{82}\mathfrak{X}_{91}\mathfrak{X}_{75}$	$\mathfrak{Z}_{(fb_8)} = \mathfrak{Z}_{66}\mathfrak{Z}_{82}\mathfrak{Z}_{91}\mathfrak{Z}_{75}$
$\mathfrak{X}_{(fb_9)} = \mathfrak{X}_{33}\mathfrak{X}_{34}\mathfrak{X}_{49}\mathfrak{X}_{50}$	$\mathfrak{Z}_{(fb_9)} = \mathfrak{Z}_{33}\mathfrak{Z}_{34}\mathfrak{Z}_{49}\mathfrak{Z}_{50}$
$\mathfrak{X}_{(fb_{10})} = \mathfrak{X}_{35}\mathfrak{X}_{36}\mathfrak{X}_{51}\mathfrak{X}_{52}$	$\mathfrak{Z}_{(fb_{10})} = \mathfrak{Z}_{35}\mathfrak{Z}_{36}\mathfrak{Z}_{51}\mathfrak{Z}_{52}$
$\mathfrak{X}_{(fb_{11})} = \mathfrak{X}_{37}\mathfrak{X}_{38}\mathfrak{X}_{53}\mathfrak{X}_{54}$	$\mathfrak{Z}_{(fb_{11})} = \mathfrak{Z}_{37}\mathfrak{Z}_{38}\mathfrak{Z}_{53}\mathfrak{Z}_{54}$
$\mathfrak{X}_{(fb_{12})} = \mathfrak{X}_{39}\mathfrak{X}_{40}\mathfrak{X}_{55}\mathfrak{X}_{56}$	$\mathfrak{Z}_{(fb_{12})} = \mathfrak{Z}_{39}\mathfrak{Z}_{40}\mathfrak{Z}_{55}\mathfrak{Z}_{56}$
$\mathfrak{X}_{(fb_{13})} = \mathfrak{X}_{41}\mathfrak{X}_{42}\mathfrak{X}_{57}\mathfrak{X}_{58}$	$\mathfrak{Z}_{(fb_{13})} = \mathfrak{Z}_{41}\mathfrak{Z}_{42}\mathfrak{Z}_{57}\mathfrak{Z}_{58}$
$\mathfrak{X}_{(fb_{14})} = \mathfrak{X}_{43}\mathfrak{X}_{44}\mathfrak{X}_{59}\mathfrak{X}_{60}$	$\mathfrak{Z}_{(fb_{14})} = \mathfrak{Z}_{43}\mathfrak{Z}_{44}\mathfrak{Z}_{59}\mathfrak{Z}_{60}$
$\mathfrak{X}_{(fb_{15})} = \mathfrak{X}_{45}\mathfrak{X}_{46}\mathfrak{X}_{61}\mathfrak{X}_{62}$	$\mathfrak{Z}_{(fb_{15})} = \mathfrak{Z}_{45}\mathfrak{Z}_{46}\mathfrak{Z}_{61}\mathfrak{Z}_{62}$
$\mathfrak{X}_{(fb_{16})} = \mathfrak{X}_{47}\mathfrak{X}_{48}\mathfrak{X}_{63}\mathfrak{X}_{64}$	$\mathfrak{Z}_{(fb_{16})} = \mathfrak{Z}_{47}\mathfrak{Z}_{48}\mathfrak{Z}_{63}\mathfrak{Z}_{64}$
$\mathfrak{X}_{(fb_{17})} = \mathfrak{X}_1\mathfrak{X}_2\mathfrak{X}_{17}\mathfrak{X}_{18}$	$\mathfrak{Z}_{(fb_{17})} = \mathfrak{Z}_1\mathfrak{Z}_2\mathfrak{Z}_{17}\mathfrak{Z}_{18}$
$\mathfrak{X}_{(fb_{18})} = \mathfrak{X}_3\mathfrak{X}_4\mathfrak{X}_{19}\mathfrak{X}_{20}$	$\mathfrak{Z}_{(fb_{18})} = \mathfrak{Z}_3\mathfrak{Z}_4\mathfrak{Z}_{19}\mathfrak{Z}_{20}$
$\mathfrak{X}_{(fb_{19})} = \mathfrak{X}_5\mathfrak{X}_6\mathfrak{X}_{21}\mathfrak{X}_{22}$	$\mathfrak{Z}_{(fb_{19})} = \mathfrak{Z}_5\mathfrak{Z}_6\mathfrak{Z}_{21}\mathfrak{Z}_{22}$
$\mathfrak{X}_{(fb_{20})} = \mathfrak{X}_7\mathfrak{X}_8\mathfrak{X}_{23}\mathfrak{X}_{24}$	$\mathfrak{Z}_{(fb_{20})} = \mathfrak{Z}_7\mathfrak{Z}_8\mathfrak{Z}_{23}\mathfrak{Z}_{24}$
$\mathfrak{X}_{(fb_{21})} = \mathfrak{X}_9\mathfrak{X}_{10}\mathfrak{X}_{25}\mathfrak{X}_{26}$	$\mathfrak{Z}_{(fb_{21})} = \mathfrak{Z}_9\mathfrak{Z}_{10}\mathfrak{Z}_{25}\mathfrak{Z}_{26}$
$\mathfrak{X}_{(fb_{22})} = \mathfrak{X}_{11}\mathfrak{X}_{12}\mathfrak{X}_{27}\mathfrak{X}_{28}$	$\mathfrak{Z}_{(fb_{22})} = \mathfrak{Z}_{11}\mathfrak{Z}_{12}\mathfrak{Z}_{27}\mathfrak{Z}_{28}$
$\mathfrak{X}_{(fb_{23})} = \mathfrak{X}_{13}\mathfrak{X}_{14}\mathfrak{X}_{29}\mathfrak{X}_{30}$	$\mathfrak{Z}_{(fb_{23})} = \mathfrak{Z}_{13}\mathfrak{Z}_{14}\mathfrak{Z}_{29}\mathfrak{Z}_{30}$
$\mathfrak{X}_{(fb_{24})} = \mathfrak{X}_{15}\mathfrak{X}_{16}\mathfrak{X}_{31}\mathfrak{X}_{32}$	$\mathfrak{Z}_{(fb_{24})} = \mathfrak{Z}_{15}\mathfrak{Z}_{16}\mathfrak{Z}_{31}\mathfrak{Z}_{32}$

5.2 Códigos Coloridos Obtidos por Tesselações Semirregulares $[2p, 2q, 2s]$ do g-toro, $g \geq 2$

Estabeleceremos aqui um processo análogo ao realizado na seção 4.2, trazendo agora um breve estudo sobre os códigos coloridos obtidos através de tesselações semirregulares estabelecidas sobre o g-toro, $g \geq 2$. Para fixar notações, vamos assumir que $p \geq q \geq s$ e que os polígonos de $2p$, $2q$ e $2s$ lados estão associados às cores vermelho, verde e azul, respectivamente.

Assim como no caso dos códigos de superfície provenientes de tesselações semirregulares, baseando-se no teorema 1.6.1, mais especificamente, no caso particular para $t = 3$ do corolário 1.6.3, dados inteiros positivos $g \geq 2$, p, q, s, R, E, V_1, V_2, V_3, tais que $R = \dfrac{4(g-1)pqs}{pqs - pq - ps - qs}$, $E = \dfrac{3R}{2}$, $V_p = \dfrac{R}{2p}$, $V_q = \dfrac{R}{2q}$ e $V_s = \dfrac{R}{2s}$, existe uma tesselação semirregular $[2p, 2q, 2s]$ do g-toro $\mathbb{M}$, a qual conta com E arestas, R vértices, $F = V_p + V_q + V_s$ faces, das quais $\dfrac{R}{2p}$ são $2p$-gons, $\dfrac{R}{2q}$ são $2q$-gons e $\dfrac{R}{2s}$ são $2s$-gons.

Observação 5.2.1. Tratando- se da tesselação semirregular $[2p, 2q, 2s]$ do g-toro $\mathbb{M}$, $g \geq 2$, tem-se:

$$\begin{aligned} \#\mathcal{F} &= \frac{2(g-1)\,(pq + ps + qs)}{pqs - pq - ps - qs}, \\ \#\mathcal{V} &= \frac{4(g-1)pqs}{pqs - pq - ps - qs}, \\ \#\mathcal{E} &= \frac{6(g-1)pqs}{pqs - pq - ps - qs}. \end{aligned}$$

Estas tesselações, quando são 3-coloríveis, fornecem códigos quânticos coloridos. A construção destes é inteiramente análoga à feita na seção 3.8.3 do capítulo 3. Assim como antes, estes códigos coloridos são construídos situando-se um qubit em cada um dos vértices da tesselação . A quantidade de qubits físicos, portanto, coincide com a de vértices da tesselação que, neste caso, é $v = \#\mathcal{V} = \dfrac{4(g-1)pqs}{pqs - pq - ps - qs}$.

Definem-se, similarmente ao já feito, dois operadores associados à cada face, os quais constituem os geradores do grupo estabilizador: Sejam $\mathcal{V}$, $\mathcal{E}$ e $\mathcal{F}$ os conjuntos de vértices, arestas e faces, respectivamente, da tesselação. Para cada $v \in \mathcal{V}$, o operador[1] $\mathfrak{X}_{(v)}$ que é aquele que atua com o operador $\mathfrak{X}$ exatamente no qubit associado ao vértice v. Analogamente define-se o operador $\mathfrak{Z}_{(v)}$. Os geradores do grupo estabilizador, o qual é denotado por $\mathcal{S}_{est}$, do código colorido são os operadores face, $\mathfrak{X}_{(f)}$ e $\mathfrak{Z}_{(f)}$, construídos da seguinte maneira:

$$\mathfrak{X}_{(f)} = \prod_{v \in f} \mathfrak{X}_{(v)}, \quad \mathfrak{Z}_{(f)} = \prod_{v \in f} \mathfrak{Z}_{(v)}.$$

[1]Utilizam-se os parêntesis na notação $\bullet_{(*)}$ para distinguir da similar utilizada nos códigos de superfície.

Denotando por $\mathcal{F}_R$, $\mathcal{F}_G$ e $\mathcal{F}_B$ os subconjuntos de $\mathcal{F}$ compostos pelas faces vermelhas, verdes e azuis, respectivamente, podemos escrever as seguintes relações:

$$\prod_{f\in\mathcal{F}_R} \mathfrak{X}_{(f)} = \prod_{f\in\mathcal{F}_B} \mathfrak{X}_{(f)} = \prod_{f\in\mathcal{F}_G} \mathfrak{X}_{(f)}, \quad \prod_{f\in\mathcal{F}_R} \mathfrak{Z}_{(f)} = \prod_{f\in\mathcal{F}_B} \mathfrak{Z}_{(f)} = \prod_{f\in\mathcal{F}_G} \mathfrak{Z}_{(f)}. \tag{5.1}$$

Observação 5.2.2. Dada uma cor $c \in \{R, G, B\}$ e um operador $A \in \{\mathfrak{X}, \mathfrak{Z}\}$, tem-se:

$$\prod_{f\in\mathcal{F}_c} A_{(f)} = \bigotimes_{v\in\mathcal{V}} A_{(v)}.$$

Proposição 5.2.3. $-Id \notin \mathcal{S}_{est}$.

Demonstração: Suponha, por absurdo, que $-Id \in \mathcal{S}_{est}$. Para tal, devem existir subconjuntos $\mathcal{F}_1, \mathcal{F}_2 \subset \mathcal{F}$ tais que $\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right) = -Id$, de onde segue que $\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)} = -\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}$.

Note que, em relação ao suporte[2] dos operadores tem-se, necessariamente, que o suporte do operador $\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)$ é não vazio ou que o suporte do operador $\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right)$ é não vazio, pois, caso contrário, $\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right) = Id$.

Vamos tratar o caso em que $sup\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right) \neq \emptyset$. O outro caso é tratado de forma análoga.

Seja v um vértice associado a um qubit do suporte de $\left(\prod_{f\in\mathcal{F}} \mathfrak{X}_{(f)}\right)$. É claro que $\left(\prod_{f\in\mathcal{F}} \mathfrak{X}_{(f)}\right)$ anticomuta com $\mathfrak{Z}_{(v)}$. Desta forma, $\left(\prod_{f\in\mathcal{F}} \mathfrak{X}_{(f)}\right)\mathfrak{Z}_{(v)} = -\mathfrak{Z}_{(v)}\left(\prod_{f\in\mathcal{F}} \mathfrak{X}_{(f)}\right)$. Com base nisto,

[2]O suporte de um operador A, no contexto em que estamos inseridos, é o conjunto dos qubits sobre os quais o operador não atua trivialmente. Eventualmente denotamos o suporte do operador A por $sup(A)$

$$\begin{aligned}
-Id &= \left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right) \\
&= Id\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right) \\
&= \mathfrak{Z}_{(v)}^2\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right) \\
&= -\mathfrak{Z}_{(v)}\left(\prod_{f\in\mathcal{F}_1} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right)\mathfrak{Z}_{(v)} \\
&= -\mathfrak{Z}_{(v)}\left(-\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}\right)\mathfrak{Z}_{(v)} \\
&= -\mathfrak{Z}_{(v)}\left(-\prod_{f\in\mathcal{F}_2} \mathfrak{Z}_{(f)}^2\right)\mathfrak{Z}_{(v)} \\
&= -\mathfrak{Z}_{(v)}\left(-Id\right)\mathfrak{Z}_{(v)} \\
&= \mathfrak{Z}_{(v)}^2 \\
&= Id,
\end{aligned}$$

de onde segue que $-Id = Id$, o que é um absurdo.□

Observação 5.2.4. O conjunto de geradores $\left\{\mathfrak{X}_{(f)}, \mathfrak{Z}_{(f)}\right\}_{f\in\mathcal{F}}$ não é independente.

De fato, das relações estabelecidas na equação 5.1, segue que $\left(\prod_{f\in\mathcal{F}_R} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_G} \mathfrak{X}_{(f)}\right) = Id$ e que $\left(\prod_{f\in\mathcal{F}_B} \mathfrak{X}_{(f)}\right)\left(\prod_{f\in\mathcal{F}_G} \mathfrak{X}_{(f)}\right) = Id$. A título de exemplo, escolhidas faces $f_r \in \mathcal{F}_R$ e $f_b \in \mathcal{F}_B$, tem-se $\mathfrak{X}_{(f_r)} = \prod_{f\in\mathcal{F}_R/\{f_r\}} \mathfrak{X}_{(f)} \prod_{f\in\mathcal{F}_G} \mathfrak{X}_{(f)}$ e, similarmente, $\mathfrak{X}_{(f_b)} = \prod_{f\in\mathcal{F}_B/\{f_b\}} \mathfrak{X}_{(f)} \prod_{f\in\mathcal{F}_G} \mathfrak{X}_{(f)}$. Observando fenômeno análogo para operadores do tipo $\mathfrak{Z}$, $\mathfrak{Z}_{(f)}$, segue que a quantidade de geradores independentes do grupo estabilizador é $2(\#\mathcal{F}_R + \#\mathcal{F}_B + \#\mathcal{F}_G) - 4$. Assim, se k é quantidade de qubits lógicos do código, temos:

$$\begin{aligned}
k &= n - (2(\#\mathcal{F}_R + \#\mathcal{F}_B + \#\mathcal{F}_G) - 4) \\
&= n - 2\#\mathcal{F} + 4 \\
&= \frac{4(g-1)pqs}{pqs - pq - ps - qs} - 2\frac{2(g-1)\,(pq + ps + qs)}{pqs - pq - ps - qs} + 4 \\
&= \frac{4(g-1)pqs}{pqs - pq - ps - qs} - \frac{4(g-1)\,(pq + ps + qs)}{pqs - pq - ps - qs} + 4 \\
&= \frac{4(g-1)pqs - 4(g-1)\,(pq + ps + qs)}{pqs - pq - ps - qs} + 4 \\
&= \frac{4(g-1)\,(pqs - pq - ps - qs)}{pqs - pq - ps - qs} + 4 \\
&= 4(g-1) + 4 \\
&= 4g.
\end{aligned}$$

Sendo $\mathcal{H} = \bigotimes_{v \in \mathcal{V}} \mathbb{C}^2$ o espaço do sistema ao qual os qubits pertencem, obviamente os operadores $\mathfrak{X}_{(f)}$ e $\mathfrak{Z}_{(f)}$ atuam sobre $\mathcal{H}$. Duas faces quaisquer $f_1, f_2 \in \mathcal{F}$, possuem zero ou dois vértices em comum, portanto, $\mathfrak{X}_{(f_1)}$ e $\mathfrak{Z}_{(f_2)}$ comutam, o que garante que $\mathcal{S}_{est}$ é abeliano.

O código colorido obtido com esta construção é $\mathcal{C}$, o subespaço vetorial de $\mathcal{H}$ obtido pela intersecção dos auto-espaços associados ao autovetor $+1$ de cada um dos operadores face:

$$\mathcal{C} = \{|\varphi\rangle \in \mathcal{H} :\ \mathfrak{X}_{(f_1)}\,|\varphi\rangle = \mathfrak{Z}_{(f_1)}\,|\varphi\rangle = |\varphi\rangle\,, f \in \mathcal{F}\}.$$

Como vimos, este código é capaz de codificar em $n = \dfrac{4(g-1)pqs}{pqs - pq - ps - qs}$ qubits físicos exatamente $k = 4g$ qubits lógicos.

Conclusão

Considerações Finais

Ao longo da jornada de estudos que culminou com a presente tese nos deparamos diversas vezes sobre linhas tênues que separam a matemática, a física, e engenharia elétrica e a ciência da computação. Em se tratando das ferramentas matemáticas, transitamos pela álgebra, quando utilizamos a noção de grupo, espaço vetorial, produto tensorial, dentre outras, e pela geometria, quando utilizamos o quociente de uma variedade diferenciável (superfície) a fim de obter uma nova variedade quociente, que na ocasião é uma superfície compacta e orientável, de característica negativa, bem como quando empregamos a geometria hiperbólica ou mesmo a riemanniana, quando induzimos uma métrica sobre as superfícies geradas pelos quocientes. Algum conhecimento sobre grafos também nos foi necessário.

Eventualmente nos deparamos com materiais e construções que estão completamente fora da nossa área de formação e de atuação.

A possibilidade de tesselar, com uma tesselação semirregular, uma superfície compacta e orientável, de característica negativa, é uma construção muito rica e interessante. Apesar de diversas tentativas frustradas, mas que muito nos enriqueceu quanto estudantes e pesquisadores, este resultado não é de nossa autoria, conforme comentado e citado em ocasião oportuna. Este resultado foi o que permitiu e serviu como substrato para o desenvolvimento das nossas ideias, as quais acoplaram as tesselações semirregulares às construções de códigos de superfície e coloridos, que num período relativamente recente foram introduzidos com o emprego de tesselações regulares.

Nos deparamos, também, com uma certa dificuldade quanto ao cálculo da distância mínima dos códigos coloridos, devido às peculiaridades que a geometria hiperbólica, mais

especificamente as tesselações nesta geometria, possuem. Com uma grande ajuda dos colegas Evandro Brizola e Waldir Soares Jr., conseguimos avançar um pouco rumo à exaustão deste problema, obtendo uma série de proposições que nos permitem controlar alguns casos particulares. Estas proposições, que foram estabelecidas na seção dos códigos coloridos provenientes de tesselações regulares estão sendo, na medida do possível e em paralelo ao presente trabalho, generalizadas para o caso em que tratamos dos códigos coloridos provenientes de tesselações semirregulares. Estas, por ainda não estarem finalizadas, não fazem parte do corpo deste trabalho. Salientamos ainda que este problema continua em aberto, embora tenhamos conjecturas a serem estudadas, sejam para serem demonstradas ou refutadas.

Como continuação imediata deste trabalho, além de fechar este problema da distância mínima para os códigos coloridos provenientes de superfícies compactas e orientáveis de característica negativa, pretendemos estudar métodos de decodificação e, posteriormente, realizar estudos de limiar de erro para os códigos aqui apresentados.

Sem sombra de dúvidas, ao fim deste processo, teremos um material muito rico e substancialmente completo acerca de códigos de superfície e coloridos construídos com tesselações hiperbólicas sobre as superfícies supracitadas.

Conclusão

Neste trabalho obtemos duas novas famílias de códigos quânticos topológicos baseados em tesselações semirregulares de superfícies compactas e conexas, com curvatura negativa constante. A primeira destas famílias consiste em códigos de superfície construídos a partir de tesselações semirregulares do g-toro, $g \geq 2$, enquanto que a segunda família consiste em códigos coloridos, também construídos a partir de tais tesselações semirregulares, porém, que são trivalentes e 3-coloríveis.

A construção e apresentação destes códigos de superfície e coloridos se encontram, respectivamente, nos capítulos 4 e 5.

No capítulo 3, no qual tratamos dos códigos quânticos coloridos construídos a partir de tesselações regulares, trivalentes e 3-coloríveis do g-toro, $g \geq 2$, mais especificamente na

seção 3.8.3, desenvolvemos uma série de proposições que fornecem um limitante superior para a distância mínima de um código colorido. Estas proposições, na medida do possível, foram generalizadas para que abarcassem os códigos coloridos provenientes das tesselações semirregulares.

Referências Bibliográficas

[1] D. Z. Albert, "On quantum-mechanical automata," Physics Letters A, vol. 98, no. 5-6, pp. 249–252, 1983.

[2] J. W. Anderson, Hyperbolic Geometry, 2nd ed. Springer, 2005.

[3] M. Atiyah, Introduction to commutative algebra. CRC Press, 2018.

[4] C. Azpurua, "A comparison of the classification of surfaces," http://math.uchicago.edu/~may/REU2019/REUPapers/Azpurua.pdf, 2019.

[5] A. F. Beardon, Algebra and geometry. Cambridge University Press, 2005.

[6] ——, The geometry of discrete groups. Springer Science & Business Media, 2012, vol. 91.

[7] P. A. Benioff, "Quantum mechanical hamiltonian models of discrete processes that erase their own histories: Application to turing machines," International Journal of Theoretical Physics, vol. 21, no. 3, pp. 177–201, 1982.

[8] H. Bombín, "An introduction to topological quantum codes," arXiv preprint arXiv:1311.0277, 2013.

[9] H. Bombín and M. A. Martin-Delgado, "Topological quantum distillation," Physical review letters, vol. 97, no. 18, p. 180501, 2006.

[10] ——, "Topological quantum error correction with optimal encoding rate," Physical Review A, vol. 73, no. 6, p. 062303, 2006.

[11] ——, "Computacion cuantica topologica y sistemas fuertemente correlacionados," Revista espanola de fisica, vol. 21, no. 2, pp. 31–45, 2008.

[12] S. Bravyi and B. Terhal, "A no-go theorem for a two-dimensional self-correcting quantum memory based on stabilizer codes," New Journal of Physics, vol. 11, no. 4, p. 043029, 2009.

[13] N. P. Breuckmann and B. M. Terhal, "Constructions and noise threshold of hyperbolic surface codes," IEEE transactions on Information Theory, vol. 62, no. 6, pp. 3731–3744, 2016.

[14] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Physical Review A, vol. 54, no. 2, p. 1098, 1996.

[15] R. G. Cavalcante, H. Lazari, J. d. D. Lima, and R. Palazzo Jr, "A new approach to the design of digital communication systems," Discrete Mathematics and Theoretical Computer Science–DIMACS Series, American Mathematical Society, Editors A. Ashikhimin and A. Barg, vol. 68, pp. 145–177, 2005.

[16] R. G. Cavalcante and R. Palazzo Jr, "Análise de desempenho de constelações de sinais geometricamente uniformes provenientes de tesselações {p,q} em espaços bidimensionais com curvatura constante," XXI Simpósio Brasileiro de Telecomunicações - SBT 04, 2004.

[17] A. Church, "A note on the entscheidungsproblem," The journal of symbolic logic, vol. 1, no. 1, pp. 40–41, 1936.

[18] ——, "An unsolvable problem of elementary number theory," American Journal of Mathematics, vol. 58, no. 2, pp. 345–363, 1936.

[19] E. B. da Silva and G. H. de Souza, "Uniform tilings, border automata and orbifolds of the hyperbolic plane," International Journal of Geometry, vol. 11, no. 1, 2022.

[20] E. B. da Silva, M. Firer, S. R. Costa, and R. Palazzo Jr, "Signal constellations in the hyperbolic plane: A proposal for new communication systems," Journal of the Franklin Institute, vol. 343, no. 1, pp. 69–82, 2006.

[21] C. D. de Albuquerque, "Análise e construção de códigos quânticos topológicos sobre variedades bidimensionais," 2009.

[22] C. D. de Albuquerque, R. Palazzo Jr, and E. B. da Silva, "Construction of topological quantum codes on compact surfaces," IEEE, pp. 391–395, 2008.

[23] ——, "Topological quantum codes on compact surfaces with genus g≥ 2," Journal of Mathematical Physics, vol. 50, no. 2, p. 023513, 2009.

[24] ——, "New classes of topological quantum codes associated with self-dual, quasi self-dual and denser tessellations," Quantum Information & Computation, vol. 10, no. 11, pp. 956–970, 2010.

[25] G. H. de Souza, "Classificação e contagem em tesselações uniformes do plano hiperbólico," 2019.

[26] N. Delfosse, "Tradeoffs for reliable quantum information storage in surface codes and color codes," in 2013 IEEE International Symposium on Information Theory. IEEE, 2013, pp. 917–921.

[27] D. Deutsch, "Quantum theory, the church–turing principle and the universal quantum computer," Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 400, no. 1818, pp. 97–117, 1985.

[28] A. L. Edmonds, J. H. Ewing, and R. S. Kulkarni, "Regular tessellations of surfaces and (p, q, 2)-triangle groups," Annals of Mathematics, pp. 113–132, 1982.

[29] ——, "Torsion free subgroups of fuchsian groups and tessellations of surfaces," Inventions mathematicae, vol. 69, pp. 331–346, 1982.

[30] ——, "Torsion free subgroups of fuchsian groups and tessellations of surfaces," Bulletin (New Series) of the American Mathematical Society, vol. 6, no. 3, pp. 456–458, 1982.

[31] R. P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, pp. 467–488, 1982.

[32] P. Giblin, Graphs, surfaces and homology: an introduction to algebraic topology. Springer Science & Business Media, 2013.

[33] M. J. Golay, "Notes on digital coding," Proc. IEEE, vol. 37, p. 657, 1949.

[34] D. Gottesman, "Class of quantum error-correcting codes saturating the quantum hamming bound," Physical Review A, vol. 54, no. 3, p. 1862, 1996.

[35] ——, "Stabilizer codes and quantum error correction," 2008.

[36] R. W. Hamming, "Error detecting and error correcting codes," The Bell system technical journal, vol. 29, no. 2, pp. 147–160, 1950.

[37] A. Hatcher, Algebraic topology. Cambridge University Press, 2005.

[38] A. Hefez and M. L. T. Villela, Códigos corretores de erros. Instituto de Matematica Pura e Aplicada, 2008.

[39] S. Katok, Fuchsian groups. University of Chicago press, 1992.

[40] A. Y. Kitaev, "Fault-tolerant quantum computation by anyons," Annals of Physics, vol. 303, no. 1, pp. 2–30, 2003.

[41] F. J. MacWilliams and N. J. A. Sloane, The theory of error correcting codes. Elsevier, 1977.

[42] C. P. Milies, "Anéis e módulos," Publicaçoes de Instituto de Matemática e Estatıstica da USP, 1972.

[43] ——, "Breve introduçao a teoria dos códigos corretores de erros," Colóquio de Matemática da Região Centro-Oeste, SBM, 2009.

[44] M. A. Nielsen and I. Chuang, "Quantum computation and quantum information," 2002.

[45] C. E. Shannon, "A mathematical theory of communication," The Bell system technical journal, vol. 27, no. 3, pp. 379–423, 1948.

[46] R. Y. Sharp, Steps in commutative algebra. Cambridge university press, 2000.

[47] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994, pp. 124–134.

[48] ——, "Scheme for reducing decoherence in quantum compueter memory," 1995.

[49] W. Smith and R. Mann, "Formation of topological black holes from gravitational collapse," Physical Review D, vol. 56, 04 1997.

[50] W. S. Soares Jr, "Novos métodos de construção de códigos quânticos coloridos sobre superfícies bidimensionais," 2017.

[51] W. S. Soares Jr and E. B. Da Silva, "Hyperbolic quantum color codes," arXiv preprint arXiv:1804.06382, 2018.

[52] A. M. Steane, "Simple quantum error-correcting codes," Physical Review A, vol. 54, no. 6, p. 4741, 1996.

[53] J. Stillwell, Geometry of surfaces. Springer Science & Business Media, 1995.

[54] A. M. Turing, "On computable numbers, with an application to the entscheidungsproblem," Proceedings of the London mathematical society, vol. 2, no. 1, pp. 230–265, 1937.

[55] W. G. Unruh, "Maintaining coherence in quantum computers," Physical Review A, vol. 51, no. 2, p. 992, 1995.

[56] J. W. Vick, Homology theory: an introduction to algebraic topology. Springer Science & Business Media, 2012, vol. 145.